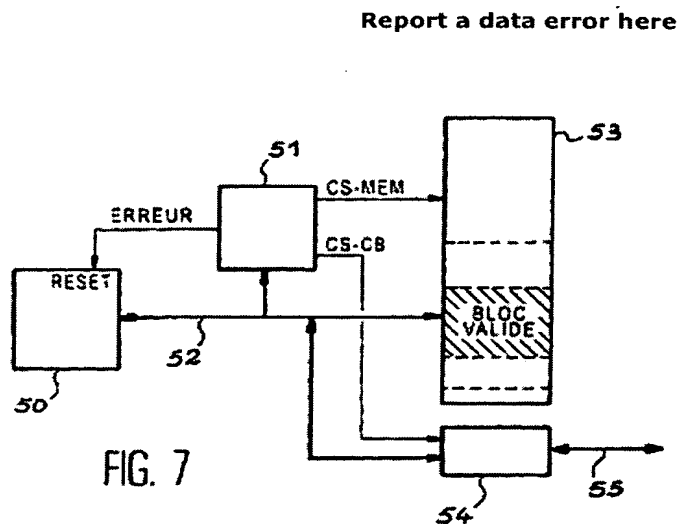


Supervision device for memory accesses

Patent number: EP1267265
Publication date: 2002-12-18
Inventor: PIGNOL MICHEL (FR)
Applicant: CENTRE NAT ETD SPATIALES (FR)
Classification:
- **International:** G06F11/00
- **European:** G06F11/14B2; G06F12/14D1
Application number: EP20020076483 19991011
Priority number(s): EP19990947525 19991011; FR19980012745 19981012

Abstract of EP1267265

The electronic system is protected from transient errors by using two time multiplexed virtual channels. Each channel (1,2) has an acquisition and processing stage which take place successively and are followed by voting, commands then scrub and standby. If an error is detected the real time cycle is inhibited and a new cycle starts using the context of the cycle before fault detection and the fault cycle acquisitions



Data supplied from the esp@cenet database - Worldwide

Rest Available Copy

FIGURE 1. ANK (USPTO)

(19)



Europäisches Patentamt

European Patent Office

Office européen des brevets



(11)

EP 1 267 265 A2

(12)

DEMANDE DE BREVET EUROPEEN

(43) Date de publication:

18.12.2002 Bulletin 2002/51

(51) Int Cl.7: G06F 11/00

(21) Numéro de dépôt: 02076483.3

(22) Date de dépôt: 11.10.1999

(84) Etats contractants désignés:

DE ES FR GB IT SE

(30) Priorité: 12.10.1998 FR 9812745

(62) Numéro(s) de document de la (des) demande(s)
initiale(s) en application de l'article 76 CBE:
99947525.4 / 1 121 642

(71) Demandeur: CENTRE NATIONAL D'ETUDES
SPATIALES
F-75039 Paris Cedex 01 (FR)

(72) Inventeur: Pignol, Michel
31000 Toulouse (FR)

(74) Mandataire: Des Termes, Monique
Société Brevatome
3, rue du Docteur Lancereaux
75008 Paris (FR)

Remarques:

This application was filed on 18.03.2002 as a
divisional application to the application mentioned
under INID code 62.

(54) Dispositif de surveillance des acces memoire

(57) La présente invention concerne un dispositif de surveillance des accès mémoire (51) dans un calculateur comprenant une unité centrale, réalisée autour d'un microprocesseur (50), et une mémoire (53), dans lequel la mémoire est partitionnée en segments, dans lequel chaque segment a un droit d'accès défini par une fonc-

tion logique de tout ou partie des clés disponibles dans le dispositif, le droit d'accès à chacun des segments étant contrôlé en temps réel, et dans lequel certains segments ont un accès autorisé seulement si le microprocesseur a une très forte probabilité d'être en bon état de fonctionnement, et permettent ainsi un stockage sûr de données critiques.

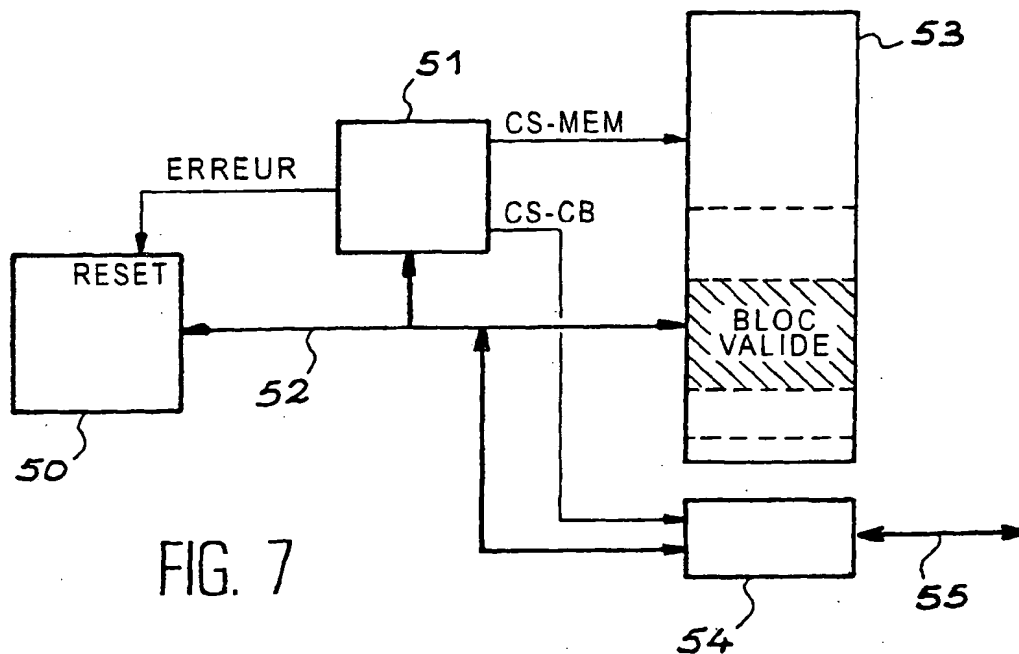


FIG. 7

EP 1 267 265 A2

Description

DOMAINE TECHNIQUE

[0001] La présente invention concerne un dispositif de surveillance des accès mémoire utilisable dans un système électronique soumis à des contraintes d'erreurs transitoires, par exemple dans le domaine spatial.

ÉTAT DE LA TECHNIQUE ANTÉRIEURE

[0002] Le dispositif de l'invention concerne toutes les architectures informatiques soumises à des erreurs transitoires. Ainsi, par exemple, les domaines suivants utilisent des calculateurs soumis à des environnements perturbants pour les composants électroniques (radiations, perturbations électromagnétiques) susceptibles d'engendrer de telles erreurs :

- domaines spatial, nucléaire et aéronautique, où l'environnement est constitué entre autre d'ions lourds,
- domaine automobile, soumis à un environnement électromagnétique sévère.

[0003] Dans la suite de la description, on considérera, à titre d'exemple, le domaine spatial du fait qu'il est très représentatif des erreurs transitoires aléatoirement générées sur des composants électroniques, et parce que c'est dans ce domaine qu'a été initialement développé et évalué le procédé de l'invention.

[0004] Les concepteurs d'architectures informatiques pour satellites sont confrontés au problème des radiations existantes dans l'espace, qui sur terre sont filtrées par l'atmosphère. Ces radiations peuvent avoir pour effet un « événement singulier » qui occasionne des changements d'états temporaires de bits dans les composants mémoires, dans les registres internes de microprocesseurs ou d'autres composants intégrés. Les erreurs engendrées par ces événements singuliers peuvent, par exemple aboutir à la génération de données erronées, par exemple une mauvaise commande d'un actuateur d'un satellite, ou à une perturbation grave du séquençement du logiciel, par exemple plantage d'un microprocesseur.

[0005] Jusqu'à présent, la solution aux erreurs de type événement singulier résidait dans l'utilisation de technologies de circuits intégrés peu sensibles à ce phénomène, dites « tolérantes aux radiations », voire insensibles, dites « durcies aux radiations ». De telles technologies, qui ne sont pas utilisées en micro-électronique industrielle, ont été développées spécifiquement pour des applications militaires et spatiales.

[0006] Le coût global associé à l'existence de ces technologies micro-électronique et au développement de composants utilisant de telles technologies, et donc le coût de vente de ces composants, est très élevé. Le ratio du coût entre un circuit durci et un circuit commer-

cial peut être de 100 ou plus.

[0007] La part de marché des composants militaires, dit « haute fiabilité », a fortement chuté, de 80% dans les années 1960 à moins de 1% en 1995. A partir de 1994, le département américain de la défense a donné un coup de frein à l'utilisation de composants électroniques militaires pour ses applications, et accéléré le processus d'appropriation par les activités militaires des spécifications/normes/composants commerciaux.

[0008] Comme décrit dans le document référencé [1] en fin de description, l'utilisation de composants électroniques commerciaux est devenu un challenge auquel est confronté le domaine spatial.

[0009] L'utilisation de composants commerciaux dans les applications spatiales est un problème auquel est confronté tout projet de nouvelle génération. Un problème majeur à résoudre est alors la sensibilité de ces composants aux radiations, et en particulier aux ions lourds : cet aspect qui était traité au niveau « composant » antérieurement, doit alors être résolu au niveau « architecture » et « système ». Comme décrit dans les deux documents référencés [2] et [3], les satellites, et donc leur électronique embarquée, sont en effet soumis à un environnement radiatif, composé de différentes particules (électrons, ions lourds, protons), que ne connaissent pas les systèmes utilisés au sol car ces particules sont filtrées par l'atmosphère.

[0010] Ces particules peuvent être dues :

- au rayonnement cosmique d'origine en partie extra galactique, en partie galactique, constitué d'ions extrêmement énergétiques,
- aux ceintures de radiation constituées d'électrons et de protons piégés engendrés suite à des interactions entre l'atmosphère terrestre et des particules solaires,
- aux éruptions solaires qui émettent des protons ou des ions lourds,
- au vent solaire généré par l'évaporation du plasma coronal, permettant l'échappement à l'attraction gravitationnelle du soleil de protons et d'ions de faible énergie.

[0011] Ces particules énergétiques, en percutant et traversant un composant électronique, lui transfèrent une partie de leur énergie qui va perturber le bon fonctionnement de celui-ci. On considère ici les problèmes nommés « événements singuliers », créés par les ions lourds et les protons.

[0012] Ces événements singuliers correspondent à la génération d'erreurs dans des cellules qui mémorisent des valeurs binaires, d'où des erreurs de bits. En règle générale, un seul bit est modifié par un ion lourd. Ces événements ne sont pas destructifs et l'on peut par la suite écrire une nouvelle donnée ; celle-ci est mémorisée sans erreur, à moins de l'apparition d'un autre événement singulier dans cette même cellule. C'est la raison pour laquelle on utilise dans la suite le terme « faute

transitoire » pour caractériser les erreurs engendrées par ces phénomènes.

[0013] Comme on l'a déjà présenté ci-dessus, la réalisation de l'électronique embarquée sur satellite est la plupart du temps réalisée avec des composants insensibles aux radiations, soit spécifiquement fabriqués pour cela, soit obtenus par sélection de composants non spécifiquement fabriqués pour cela.

[0014] Pour pouvoir utiliser des composants commerciaux dans le domaine spatial sur une large échelle, une première possibilité est une sélection par test en radiation systématique des composants commerciaux. Une telle méthode serait non seulement très coûteuse sur le plan de la sélection, mais encore un pis aller car elle ne permet pas forcément d'utiliser les grands standards de l'industrie, ce qui est pourtant souhaitable.

[0015] Une deuxième possibilité économiquement plus rentable permet de réduire les contraintes sur les choix de composants. Elle consiste à trouver une méthode permettant de tolérer les phénomènes engendrés par les radiations, en particulier les erreurs transitoires, c'est-à-dire définir des architectures permettant de détecter les erreurs, puis de les corriger. La prise en compte des fautes transitoires est alors transférée du niveau « composant » au niveau « architecture » et « système ».

[0016] Un ensemble de mécanismes de détection, isolation et recouvrement de fautes est décrit dans les documents référencés [4], [5] et [6]. Certains mécanismes permettent simplement de détecter des erreurs, d'autres de les détecter puis de les masquer, voire de les corriger. Par ailleurs, ces mécanismes sont adaptés au traitement soit de fautes temporaires, soit de pannes définitives, soit des deux.

[0017] Un rappel succinct de mécanismes usuels est proposé ci-dessous, avec quelques exemples d'application en particulier dans le domaine spatial :

- Evitement de fautes : rafraîchissement systématique des données statiques avant leur utilisation effective ; autotests dits « off-line » (en dehors du fonctionnement nominal) permettant de détecter une panne de composant avant que celui-ci ne soit utilisé.
- Codes détecteurs ou détecteurs/correcteurs d'erreurs qui s'appliquent aux mémoires, aux communications, et éventuellement à la logique, essentiellement dans la réalisation de circuits intégrés spécifiques d'une application (ASIC) ou de circuits logiques programmables par l'utilisateur (FPGA) à contrôle intégré. Des circuits à détection et correction d'erreurs (EDAC) sont systématiquement utilisés en spatial sur les plans mémoire. Une fonction de relecture systématique (ou « scrubbing ») de tout le plan mémoire est associée à ces circuits et s'exécute en tâche de fond afin d'éviter l'accumulation d'erreurs dormantes qui, à terme, pourraient mettre en défaut la possibilité de détection/correc-

tion.

- Duplication et comparaison, ou triplification et vote majoritaire (« N Modular Redondance », redondance modulaire d'ordre N). Ces mécanismes permettent d'obtenir des architectures sûres (« fail safe ») lors d'une panne qui ne généreront pas de mauvaise commande mais qui s'arrêteront à la première faute (duplex), ou des architectures restant opérationnelles (« fail operational ») lors d'une panne, qui auront la capacité de masquer une erreur simple en temps réel et de poursuivre en restant « sûres » (triplex). On trouve également dans cette classe les architectures maître/contrôleur où l'on duplique uniquement les microprocesseurs, les données sortant du « maître » étant vérifiées par le « contrôleur » ; le microprocesseur ERC-32 de la société MHS S.A. intègre un tel mécanisme.
- Méthode de programmation multiple (« N-version programming »), associée aux architectures à redondance modulaire d'ordre N, qui permet de détecter également des erreurs de conception logicielle. Chaque calculateur dispose d'une version de logiciel qui a été développée spécifiquement à partir d'une spécification commune.
- Redondance temporelle : il s'agit soit d'avoir deux exécutions successives suivies d'une comparaison, soit d'avoir une seule exécution suivie du chargement d'un registre de commande puis de la relecture de celui-ci afin de réaliser une comparaison et une validation, tel le mécanisme « armer puis tirer » utilisé en spatial pour les commandes très critiques, par exemple le déclenchement des éléments pyrotechniques.
- Contrôle du temps d'exécution : des « chiens de garde », compteurs de temps qui permettent de vérifier l'exécution en une durée bornée d'un logiciel, sont utilisés dans tous les calculateurs spatiaux. De plus, des contrôles plus fins du temps d'exécution peuvent être incorporés dans le logiciel : contrôle de la durée d'une tâche, durée maximale autorisée pour obtenir la réponse d'un élément de communication, etc. Des logiciels permettent de positionner des contrôles sur la durée d'exécution des tâches.
- Vérification du flot de contrôle, par exemple contrôle du séquençement d'un microprocesseur. Les chiens de garde permettent un contrôle grossier : détection d'un plantage dur. Un contrôle fin du flot d'instruction est possible avec un processeur de surveillance plus ou moins complexe. Le contrôle par analyse de signature est particulièrement efficace et peu demandant en électronique. Ce concept a été intégré dans l'ERC-32 de la société MHS S.A. mais, pour être transparent à l'utilisateur, il a fallu développer un compilateur spécifique qui calcule les signatures de référence et les intègre dans le code.
- Contrôle de la validité de l'adressage d'un microprocesseur à partir des droits d'accès par pages/

segments.

- Contrôle de vraisemblance : ce principe est utilisé dans les Systèmes de Contrôle d'Attitude et d'Orbite (ou SCAO) de satellites où l'on compare soit les données de plusieurs types de capteurs pour détecter des incohérences éventuelles, soit une donnée par rapport à une référence estimée grâce à un filtre prédictif sur les valeurs précédentes, soit une donnée par rapport à une plage d'appartenance prédéfinie. Les méthodes dites « tolérance aux fautes basée sur le traitement algorithmique » représentent une sous-classe des contrôles de vraisemblance, la vérification étant basée sur l'exécution d'un deuxième algorithme, par exemple l'algorithme inverse qui permet de retrouver les données initiales en partant des résultats obtenus si ceux-ci sont exempts d'erreurs.
- Contrôle structurel ou sémantique des données, nécessitant des structures de données relativement complexes.
- Concepts complémentaires de recouvrement d'erreurs, principalement des points de reprise pour les mécanismes décrits précédemment ne permettant pas de corriger les fautes : sauvegarde régulière de contextes et reprise à partir du dernier contexte sauvegardé.
- Une autre possibilité du recouvrement d'erreurs réside en la réinsertion d'une ressource en faute par transfusion d'un contexte sain dans un calculateur fautif, afin de retrouver la capacité initiale de détection/correction.

[0018] Il existe également des documents de l'art connu dans le domaine de la redondance temporelle.

[0019] Le document référencé [5] évoque la possibilité d'exécuter une tâche trois fois de suite et de « voter » le résultat.

[0020] La possibilité de réaliser un fonctionnement de type redondance modulaire d'ordre N en logiciel, est également mentionnée de façon théorique dans le document référencé [6].

[0021] Dans ce dernier document, une autre méthode permet de discriminer les fautes transitoires des fautes permanentes voire de les corriger. La détection n'est pas une méthode de redondance temporelle mais, par exemple, un codage des données. En cas de détection, le traitement est exécuté une deuxième fois ; si la deuxième exécution donne des résultats sans erreur, il s'agit d'une erreur transitoire et il est inutile de reconfigurer le système ; dans le cas inverse, une reconfiguration est nécessaire car il s'agit d'une faute permanente.

[0022] Dans ces deux documents, la redondance temporelle est mentionnée comme théoriquement possible, mais aucune information n'est fournie quant à la possibilité réelle de sa réalisation, aucun développement concret n'est cité. Certains problèmes restent entiers : en particulier, le vote peut-il être réalisé par le

microprocesseur lui-même ou doit-il être réalisé par un organe externe et indépendant du microprocesseur. En effet, le résultat du vote se doit d'être robuste puisque c'est l'élément décisionnel, or le microprocesseur peut être victime de dysfonctionnement : erreur de données, plantage du séquençement, etc. La réalisation du vote par le microprocesseur est donc un élément majeur non abordé. Par ailleurs, la granularité sur laquelle se base la détection n'est pas définie.

- 10 [0023] Le document référencé [7] est un peu plus concret. Il présente une évaluation comparative de deux méthodes de détection d'erreurs. L'une d'entre elles est nommée « triple redondance modulaire logicielle ». La triple redondance modulaire est considérée comme habituellement réalisée en matériel. La méthode évaluée dans cette publication utilise la redondance temporelle par exécution successive du logiciel, tous les modules, notamment le module vote, étant réalisés en logiciel et exécutés sur le même microprocesseur. C'est donc une approche purement logicielle. La figure 1, qui correspond à la figure 1 de ce document, illustre la réalisation de la détection : trois modules vote 1, 2 et 3 comparant chacun les résultats de l'exécution de trois traitements 4, 5 et 6 sont suivis d'un étage de décision 7, qui compare le résultat issu de chacun des modules votes pour vérifier la cohérence des trois traitements. La triple redondance modulaire logicielle est programmée sur un microprocesseur MC68000. Environ 1500 erreurs ont été injectées pour valider ce logiciel. La mémoire n'est pas protégée des erreurs par un circuit de détection et correction d'erreurs. Ce document conclut que seules les erreurs qui entraîneraient un traitement à en perturber un autre, ne peuvent pas être détectées. De plus, les erreurs affectant les communications entre programmes ne sont pas entièrement tolérées.

35 [0024] Ce document mentionne une réalisation concrète d'une architecture où les traitements sont exécutés trois fois de suite (redondance temporelle), et où le module vote est exécuté trois fois, les résultats des modules de vote étant ensuite eux-mêmes votés. Il apparaît que le vote n'est aucunement sécurisé, c'est pour cela qu'il doit être tripliqué. La prise finale de décision est alors confiée au dernier étage illustré sur la figure, qui est indirectement sécurisé par le fait qu'il est forcé-
45 ment d'une taille très faible (il suffit de quelques lignes de code pour voter trois données) : statistiquement, les événements singuliers affectant directement ce module sont négligeables, mais ceci ne le sécurise pas vis-à-vis des erreurs de séquençement du microprocesseur.

50 [0025] Le document référencé [8] présente également une réalisation de « triple redondance modulaire logicielle » sur un microprocesseur de type iAPX 432, réalisation proche de celle présentée dans le document référencé [7] : chaque sous-tâche logicielle est exécutée trois fois de suite, puis un module de vote logiciel est également exécuté trois fois, ce qui permet de conclure qu'il n'est pas sécurisé, ces tâches s'exécutant sur le même microprocesseur de façon asynchrone. Une

phase d'injection d'erreur a permis de mettre en évidence des propagations d'erreurs entre sous-tâches, ce qui tend à montrer qu'il n'y a pas d'étanchéification des sous-tâches les unes par rapport aux autres.

[0026] Le document référencé [9] donne un aperçu général de procédé de traitement de système électronique ou digital soumis à des contraintes d'erreurs transitoires et mentionne, comme moyens de traitement, la redondance d'ordre spatiale ainsi que la redondance d'ordre temporelle.

[0027] Le document référencé [10] divulgue également un procédé de traitement d'un système électronique soumis à des erreurs, ledit système proposant l'utilisation d'une seule chaîne physique afin d'éviter l'utilisation de chaînes redondantes.

[0028] Le document référencé [11] décrit des procédés appliqués aux microprocesseurs récents pour permettre une gestion mémoire et une mémoire virtuelle. Un principe d'accès limité aux informations est envisagé. Certains droits d'accès à une page ou à un segment sont donnés à chaque processus, ces droits d'accès étant contrôlés en temps réel.

[0029] Une estimation du taux d'événements singuliers dans un calculateur spatial typique a été réalisée ; ce taux dépend bien sûr d'hypothèses comme du nombre de cellules mémoire et de la valeur de la sensibilité d'une cellule unitaire prise en compte. Une simulation de la criticité des erreurs sur la gestion de l'attitude d'un satellite a également été faite en prenant en compte la génération d'une mauvaise commande sur un actuateur moyennement critique d'un système de contrôle d'attitude et d'orbite, par exemple une roue à réaction. Il apparaît que le taux d'événements singuliers est faible, mais pas suffisamment pour négliger ce phénomène vis-à-vis de deux types de commandes :

- commandes les plus critiques : pyrotechnie, propulseurs, gestion batterie, etc. On ne peut pas prendre le risque de perdre un satellite plusieurs fois par an ;
- commandes moyennement critiques : roues à réaction, magnéto-coupleurs, etc. Certaines missions, en particulier commerciales (observation, télécommunication) ne sont pas compatibles de perturbations d'attitudes potentiellement engendrées par ces erreurs, même si celles-ci restent limitées.

[0030] Par ailleurs, la fréquence des événements singuliers est très largement supérieure à la fréquence du cycle temps réel du calculateur.

[0031] L'objet de l'invention est de proposer un dispositif de surveillance des accès mémoire utilisable dans un système électronique soumis à des contraintes d'erreurs transitoires permettant d'utiliser des composants commerciaux malgré leur sensibilité aux événements singuliers, en permettant de détecter l'apparition d'erreurs transitoires et de les corriger.

EXPOSÉ DE L'INVENTION

[0032] La présente invention concerne un dispositif de surveillance des accès mémoire (SAM) dans un calculateur, comprenant notamment une unité centrale réalisée autour d'un microprocesseur, et une mémoire, caractérisé en ce que la mémoire est partitionnée en segments, et en ce que chaque segment a un droit d'accès défini par une fonction logique de tout ou partie des clés disponibles dans le dispositif, le droit d'accès à chacun des segments étant contrôlé en temps réel. Certains segments ont un accès autorisé seulement si le microprocesseur a une très forte probabilité d'être en bon état de fonctionnement, permettant ainsi un stockage sûr de données critiques (par exemple des données de contexte).

[0033] Avantageusement, en fonction de la programmation des clés disponibles dans le dispositif, un ensemble de segments disjoints est accessible, en lecture seule pour certains segments, en lecture/écriture pour d'autres segments.

[0034] Avantageusement, la taille des segments est quelconque, afin d'être optimisée pour une application donnée.

[0035] Avantageusement, la définition du jeu de clés disponibles, les fonctions logiques de combinaison de ces clés et la configuration des segments accessibles en fonction de la programmation des clés, sont spécifiques.

[0036] On peut, de plus, définir les spécificités de ce dispositif liées à la propre définition des clés, par exemple :

- l'un des segments dispose d'une autorisation d'écriture accessible selon un état exceptionnel du calculateur, permettant ainsi un stockage sûr de données critiques (par exemple le code),
- les segments permettant un stockage sûr de données critiques sont groupés par deux (segment "ancien" et segment "nouveau") et travaillent en basculement (en "flip-flop").

[0037] Le dispositif de l'invention permet de réaliser :

- une duplication temporelle de l'exécution des tâches, et vote des tables résultantes,
- une détection de toutes les erreurs de données grâce au vote des tables,
- une détection des erreurs de séquençement grâce aux dispositifs matériels et logiciels de sécurisation du vote et de contrôle des droits d'accès ;
- une correction transparente à l'application : tout se passe comme s'il y avait un « trou » d'un cycle temps réel.

[0038] La minimisation des développements spécifiques est l'un des avantages du traitement d'erreur autorisé par le dispositif de l'invention, à savoir :

- Pour le logiciel :
 - le regroupement des variables votées dans des tables,
 - le module de « Vote et génération des commandes », qui est par ailleurs réutilisable d'une application à l'autre,
 - la gestion du procédé de l'invention (gestion de la duplication temporelle, des dispositifs matériels de surveillance des accès mémoire et de fenêtre de validation temporelle, de la correction des erreurs).
- Pour le matériel :
 - la surveillance des accès mémoire et la fenêtre de validation temporelle : ce sont des composants simples, qu'il faut intégrer dans un circuit FPGA ou, mieux, dans le circuit ASIC associé usuellement au microprocesseur (décodage d'adresses, etc.), ils sont par ailleurs réutilisables d'une application à l'autre,
 - la protection de l'électronique des commandes critiques par des mécanismes usuels de tolérance aux fautes (e.g. instrumentation).

[0039] Les avantages du traitement d'erreur autorisé par le dispositif de l'invention sont donc les suivants :

- Très peu de développement matériels,
- Très peu de développement logiciels,
- Minimisation des coûts récurrents (un seul calculateur) par rapport à d'autres architectures tolérantes aux fautes,

de telles caractéristiques étant inhabituelles dans le domaine de la tolérance aux fautes.

[0040] De plus l'utilisation de composants « commerciaux » dans le spatial présente les principaux avantages suivants :

- Résoudre le problème de la réduction constatée de l'offre en composants « haute fiabilité », suite aux retraits de ce marché de fournisseurs majeurs.
- Réduction des coûts, aspect stimulé par le contexte budgétaire. Or, le poste « composants haute fiabilité » est non négligeable dans le coût total du développement d'un équipement, et devient prépondérant dans son coût récurrent.
- Utilisation de fonctions/composants plus performants, permettant de réduire le volume d'électronique et/ou d'augmenter la fonctionnalité.
- Réduction de la durée de développement des projets pour offrir un accès à l'espace plus réactif, le

délai d'approvisionnement des composants « haute fiabilité » étant couramment de un ou deux ans.

- 5 **[0041]** Avantageusement, le dispositif de l'invention a une vocation générique, et peut être utilisé dans tout type de calculateur soumis à des contraintes d'erreurs transitoires, quelle que soit l'origine de ces erreurs (radiations cosmiques, impulsion électromagnétique, etc.),
- 10 mais il s'applique tout naturellement au domaine spatial.

BRÈVE DESCRIPTION DES DESSINS

- 15 **[0042]**
- la figure 1 illustre une réalisation de triple redondance modulaire logicielle de l'art connu,
 - la figure 2 illustre le synoptique de l'architecture matérielle servant de référence dans la présente description,
 - la figure 3 illustre le diagramme temporel de l'architecture logicielle de référence,
 - la figure 4 illustre le séquençement de l'architecture de référence,
 - 25 • les figures 5A et 5B illustrent le séquençement global de fonctionnement : respectivement sans utiliser, et en utilisant le traitement d'erreur autorisé par le dispositif de l'invention,
 - la figure 6 illustre une description fonctionnelle du traitement d'erreur autorisé par le dispositif de l'invention,
 - la figure 7 illustre le synoptique de l'ensemble de l'architecture matérielle du traitement d'erreur autorisé par le dispositif de l'invention,
 - 35 • la figure 8 illustre la zone de confinement des erreurs au niveau matériel,
 - la figure 9 illustre le séquençement du traitement d'erreur autorisé par le dispositif de l'invention et le basculement des tables de contexte,
 - 40 • la figure 10 illustre le vote des données,
 - les figures 11A et 11B illustrent la structure du vote du traitement d'erreur autorisé par le dispositif de l'invention : respectivement les différentes erreurs de séquençement de type « plantage doux » et la structure de la procédure de vote/génération des commandes.
- 45

EXPOSÉ DÉTAILLÉ DE MODES DE RÉALISATION PARTICULIERS

50 **[0043]** Dans la suite de la description, on considère à titre d'exemple une application du dispositif de l'invention dans le domaine spatial.

55 **[0044]** Une application typique et générique d'un calculateur utilisé en spatial est fournie ci-dessous, tant du point de vue matériel que logiciel. L'architecture de référence, illustrée sur la figure 2, sert de base à la description du dispositif de l'invention.

[0045] L'unité de gestion de bord 10, illustrée sur cette figure 2, comprend :

- une unité centrale 11 réalisée autour d'un microprocesseur,
- une mémoire de masse 12
- des interfaces puissance 13, charge utile 15, pyrotechnie 16, thermique 17, système de contrôle d'attitude et d'orbite 18,
- reliés par un bus de données 19,
- un interface télécommande-télémessure 14
- une électronique de surveillance et de reconfiguration 20,
- des convertisseurs continu-continu 21 délivrant des alimentations commutées AC et permanentes AP.

[0046] L'interface puissance 13 est reliée à un générateur solaire 25 et à une batterie 26.

[0047] L'interface télécommande-télémessure 14 est relié à un émetteur/récepteur, duplexeur 27 en liaison avec des antennes 28 et 29.

[0048] La charge utile 31 est reliée à l'unité centrale 11 par un bus avionique 32, à la mémoire de masse 12 ainsi qu'à l'interface télécommande/télémessure 14 par une liaison série haut débit 33, à l'interface charge utile 15.

[0049] L'interface pyrotechnie 16 est relié à des systèmes déployables 35.

[0050] L'interface thermique 17 est reliée à des réchauffeurs, thermistances 36.

[0051] L'interface système de contrôle d'attitude et d'orbite 18 est relié à des capteurs C1, C2, ... Cn, à des actionneurs A1, A2 ... Am, et à un capteur de pression des réservoirs 37.

[0052] Une telle architecture est donc constituée de différents modules de traitement (module unité centrale) ou d'entrée/sorties (modules d'acquisition, modules de commande). Les modules d'entrée/sortie intègrent l'électronique de bas niveau (convertisseur analogique/numérique ou numérique/analogique, multiplexeurs de voies numériques ou analogiques, relais, etc.).

[0053] Les modules peuvent indifféremment être des cartes reliées par un bus fond-de-panier, ou des boîtiers complets reliés par un bus avionique. Dans les deux cas, l'interface au bus est réalisé par un Coupleur de Bus (CB) maître sur le module Unité Centrale, et par des coupleurs de bus abonnés sur les autres modules.

[0054] L'architecture logicielle de référence, comme illustrée sur la figure 3, est constituée de tâches de traitement (par exemple : tâche du système de contrôle d'attitude et d'orbite, tâche contrôle thermique, tâche horloge temps réel, tâche gestion bord, etc.), chaque tâche générant des résultats qui doivent sortir du calculateur (commandes ou cdes), ces résultats étant générés (i.e. sortis du calculateur) au fur et à mesure de leur calcul. Les acquisitions (ou Acq) sont groupées en début de cycle temps réel pour raison de cohérence temporelle (système de contrôle d'attitude et d'orbite par

exemple).

[0055] Sur la figure 3 les tâches A, B et C sont représentées à la même fréquence pour des raisons de clarté de la description.

- 5 **[0056]** L'activité de ces tâches est rythmée par un cycle temps réel déclenché par une interruption Temps Réel IT-TR cyclique. Ce cycle permet de démarrer de façon cyclique certaines tâches, qui travaillent soit à la fréquence du cycle temps réel, soit à une sous-fréquence. D'autres tâches sont asynchrones, initialisées sur événements.
- 10

[0057] Une représentation faisant à la fois apparaître l'architecture de référence matérielle et logicielle est fournie à la figure 4. Sur cette figure sont représentées l'unité centrale 40, l'électronique d'acquisition 41 reliée à des capteurs 42, et l'électronique de commande 43 reliée à des actionneurs 44, ces deux électroniques 41 et 43, ainsi que l'unité centrale étant reliées à un bus de données 45.

15

20 **[0058]** Le séquençement des trois phases principales Ph1, Ph2 et Ph3, que sont l'acquisition de données, leur traitement, et la génération de commandes, mettent en jeu les trois parties distinctes de l'électronique 40, 41, 43, les phases Ph2 et Ph3 étant imbriquées.

25 **[0059]** La partie matérielle de cette architecture ne se base que sur des blocs fonctionnels et ne tient donc pas compte de la spécificité de composants particuliers et de leurs capacités éventuelles dans le domaine de la détection/correction d'erreur. Le dispositif de l'invention est donc autosuffisant. Cependant, l'utilisation d'éventuels mécanismes de tolérance aux fautes intégrés aux composants retenus pour une application donnée ne peut qu'améliorer le taux de couverture d'erreurs par rapport au traitement d'erreur autorisé par le dispositif de l'invention seul.

30

35 **[0060]** Une détermination des signatures d'erreurs potentielles de l'architecture de référence soumise à des événements singuliers a été réalisée. Elle a permis de regrouper les erreurs en deux classes essentielles :

40

- les erreurs de données,
 - les erreurs de séquençement, qui peuvent être également partagées en deux sous-classes :
- 45
- « plantage doux » : branchement erroné, mais le microprocesseur retombe en phase avec les instructions, et poursuit un séquençement des instructions plus ou moins erratique ;
- 50
- « plantage dur » : le microprocesseur n'est plus opérationnel ; par exemple le microprocesseur ne reste pas en phase avec les instructions, le microprocesseur charge le registre d'instructions avec des données, le pointeur de pile est perturbé, blocage du séquençement des instructions, attente d'un événement impossible, boucle infinie, etc.
- 55

[0061] Ces deux classes se subdivisent elles-mêmes en différentes sous-classes, dont la plus importante concerne les erreurs d'adresses.

[0062] La distinction entre plantage « doux » et « dur » est importante : autant un dispositif matériel externe au microprocesseur est généralement nécessaire à la détection des plantages « durs » (e.g. un chien de garde), autant un mécanisme logiciel peut être suffisant pour détecter un plantage « doux » puisque, dans ce dernier cas, le microprocesseur continue à exécuter du code, même si c'est de façon erratique.

[0063] Par ailleurs, les plantages du microprocesseur constituent une classe d'erreurs critiques, car un « microprocesseur fou » est capable d'actions pouvant avoir des conséquences catastrophiques pour une mission spatiale ; il est donc important de s'attacher à les détecter, et ceci avec un temps de latence court, et/ou de réaliser des zones de confinement d'erreurs afin de minimiser la probabilité de mauvaises commandes suite à une erreur non détectée.

[0064] On va à présent décrire le fonctionnement du dispositif de l'invention proprement dit et du traitement d'erreur qu'il autorise.

[0065] De façon globale, la granularité utilisée pour la détection/correction est le cycle temps réel de base du calculateur, par exemple le cycle de la tâche du système de contrôle d'attitude et d'orbite d'un calculateur de plate-forme.

[0066] En effet, dans le traitement d'erreur autorisé par le dispositif de l'invention comme dans un duplex structurel, l'objectif est de laisser le calculateur travailler sans surveillance et de choisir ou « voter » uniquement les données qui doivent sortir du calculateur (les commandes) ou qui servent à la correction (le contexte).

[0067] Le choix du cycle temps réel pour la granularité présente de nombreux avantages :

- c'est à cette fréquence que l'on accède en acquisition ou en commande à une majorité de capteurs/actuateurs ;
- c'est en fin de cycle temps réel que l'on dispose de données « actives » en nombre relativement restreint : il n'y a pas de multiples données intermédiaires, ni de variables locales en cours d'utilisation :
 - pour la détection, on les stocke en un jeu de tables qui sont votées,
 - pour la correction, on dispose d'un contexte de reprise simple et bien localisé.

[0068] De façon plus précise, la granularité de la détection/correction pour une tâche donnée est la fréquence de cette même tâche, puisque le vote se fait en fin de tâche. Par conséquent, si l'on considère une tâche du système de contrôle d'attitude et d'orbite à 10 Hz et

une tâche thermique à 1 Hz, la granularité est de 10 Hz pour le système de contrôle d'attitude et d'orbite et de 1 Hz pour la thermique. Pour raison de clarté, on conserve dans la suite du document la notion de « granularité par cycle temps réel » plutôt que « par tâche ».

[0069] Pour bénéficier de l'efficacité du duplex, (deux chaînes identiques en parallèle, exécutant le même logiciel, avec comparaison des sorties), qui permet de détecter toutes les erreurs sans exception quel que soit leur type (erreur de données, d'adresses, de séquençement, de configuration, etc.), tout en supprimant la redondance structurelle, le traitement d'erreur autorisé par le dispositif de l'invention consiste à implanter un fonctionnement duplex sur une seule chaîne physique. Dans un cycle temps réel donné, on multiplexe dans le temps deux chaînes virtuelles implantées sur une seule chaîne physique : les données résultantes de chaque exécution d'une chaîne virtuelle sont stockées dans des « tables du duplex multiplexé dans le temps » (e.g. commandes, contexte) afin d'être votées avant utilisation.

[0070] La correction consiste, suite à une détection, à inhiber le cycle temps réel en cours, et à recharger un contexte sain pour effectuer une reprise qui consiste en une exécution nominale du cycle suivant à partir du contexte rechargé : tout se passe comme s'il y avait un « trou » d'un cycle temps réel.

[0071] Le traitement d'erreur autorisé par le dispositif de l'invention est basé sur le fait qu'une erreur générée par un événement singulier est transitoire : une telle erreur apparaissant pendant l'exécution de la première chaîne virtuelle n'est pas reproduite lors de l'exécution de la deuxième chaîne (ou réciproquement). Par contre, les erreurs statiques dans le temps ne peuvent être détectées par le traitement d'erreur autorisé par le dispositif de l'invention : par exemple les pannes de composants (collage d'un bit, etc.), voire même certaines erreurs dues à des événements singuliers et qui provoqueraient une erreur permanente (e.g. blocage d'un séquenceur).

[0072] Les actions en aval du module vote, c'est-à-dire le transfert de données vers l'électronique de commande (i.e. le bus de données), ainsi que l'électronique de commande elle-même, ne sont pas protégées par le traitement d'erreur autorisé par le dispositif de l'invention. L'utilisateur réalise une analyse système afin de déterminer les commandes critiques qui nécessitent d'être exemptes d'erreurs, et de les protéger par des mécanismes bien connus de l'homme de métier : codage des données, circuit d'auto-contrôle, instrumentation de l'électronique de commandes, etc.

[0073] La figure 6 donne une description fonctionnelle du traitement d'erreur autorisé par le dispositif de l'invention.

[0074] Sur cette figure on retrouve les flux de données (traits gras) grâce auxquels la chaîne virtuelle #1 47 reçoit les acquisitions #1, la chaîne virtuelle #2 48 reçoit les acquisitions #2, le voteur sécurisé 49 reçoit les sor-

ties de ces deux chaînes 47 et 48, et émet les commandes. On retrouve également le signal d'erreurs (trait fin) qui relie le module vote sécurisé 49 aux deux chaînes virtuelles 47 et 48, pour réaliser une demande de rechargement de contexte afin d'initialiser une correction par reprise.

[0075] Le séquençement global du traitement d'erreur autorisé par le dispositif de l'invention est illustré sur les figures 5A et 5B :

- figure 5A : séquençement sans le traitement d'erreur autorisé par le dispositif de l'invention, les commandes étant néanmoins groupées en fin de traitement,
- figure 5B : séquençement avec le traitement d'erreur autorisé par le dispositif de l'invention.

[0076] La figure 5A illustre deux cycles temps réels N et N+1, et le début du cycle N+2.

[0077] Chaque cycle temps réel est constitué de quatre phases distinctes dans le temps :

- acquisition des données,
- traitement avec calcul des commandes,
- transmission des commande,
- tâche de fond (« Scrub ») et veille (« Standby ») appelée ici « Scrub+Standby ».

[0078] La figure 5B illustre le traitement d'erreur autorisé par le dispositif de l'invention, dans lequel chaque cycle temps réel est constitué de :

- acquisition chaîne virtuelle numéro 1 (ChV#1),
- traitement chaîne virtuelle numéro 1 ; les résultats étant stockés dans une table TAB#1,
- acquisition chaîne virtuelle numéro 2 (ChV#2),
- traitement chaîne virtuelle numéro 2 ; les résultats étant stockés dans une table TAB#2,
- vote des tables TAB#1 et TAB#2,
- génération des commandes
- tâche de fond et veille.

[0079] La figure 7 illustre un synoptique de l'ensemble du traitement d'erreur autorisé par le dispositif de l'invention, en présentant l'ensemble des circuits permettant une mise en oeuvre de celui-ci.

[0080] Un premier module microprocesseur 50 permettant de gérer l'ensemble des mécanismes logiciels, en particulier :

- la duplication temporelle des tâches,
- la mise en table des variables,
- le vote sécurisé,
- la correction par reprise,
- la gestion des mécanismes matériels.

[0081] Le dispositif de l'invention 51 de surveillance d'accès mémoire et de fenêtre de validation temporelle est relié au bus 52 du microprocesseur 50, une mémoire à détection et correction d'erreur 53 et un coupleur de bus 54.

[0082] Le module 51 représentant le dispositif de l'invention génère un signal d'erreur sur la borne « Reset » du microprocesseur 50, un signal de sélection (« chip-select », CS) sur la mémoire 53, et un signal de sélection sur le coupleur de bus 54.

[0083] La mémoire 53 est partagée en segments, chaque segment disposant d'un droit d'accès spécifique (validation par clés). Le coupleur de bus 54, qui est relié à un bus de données 55 donnant accès aux autres fonctions du calculateur (électronique d'acquisition, de commande, etc..) est validé par un signal de type « fenêtre temporelle ».

[0084] Le traitement d'erreur autorisé par le dispositif de l'invention s'articule ainsi autour des caractéristiques suivantes :

- de trois niveaux de zones de confinement des erreurs : temporel, logiciel et matériel ;
- d'une mise en table des variables/données ;
- d'une duplication temporelle des traitements ;
- d'un module vote logiciel sécurisé unique permettant une détection d'erreur par comparaison des résultats de chacun des traitements, le module vote réalisant également la génération des commandes ;
- d'un processeur de surveillance logiciel qui participe au contrôle de l'intégrité du vote ;
- d'un plan mémoire de l'unité centrale protégé des événements singuliers par code détecteur et correcteur d'erreur ;
- d'une segmentation de la mémoire associée au dispositif matériel de contrôle des droits d'accès qui, avec l'élément précédent, permet de sauvegarder de façon sûre le contexte de reprise et de détecter des erreurs d'adressage ;
- d'un contrôle des transferts vers l'électronique de

commande, via le bus de données, par le dispositif matériel contrôlant les droits d'accès, délimitant ainsi une zone de confinement des erreurs ;

- d'une correction par reprise, en cas d'erreur.

[0085] On va, à présent analyser successivement chacune de ces caractéristiques.

Zones de confinement

[0086] La zone majeure de confinement des erreurs 60 est constituée de l'électronique d'acquisition 41 et de l'unité centrale 40, comme illustré sur la figure 8 : sur cette figure on utilise les mêmes références que celles de la figure 4. Ainsi, si une erreur perturbe les acquisitions ou le traitement, cette erreur ne peut pas être générée vers l'électronique de commande 43. Les erreurs survenant suite à un événement singulier dans l'électronique d'acquisition 41 ou dans l'unité centrale 40 ne peuvent donc pas engendrer de mauvaises commandes du satellite ; elles ne perturbent pas la mission.

[0087] Cette zone de confinement 60 est, grâce au vote, effective pour les erreurs que le module vote est capable de détecter. Pour les autres erreurs, cette zone de confinement est également quasi étanche grâce à la présence du contrôle de droit d'accès : le dispositif matériel de fenêtre de validation temporelle bloque toute génération de commande sur le bus non autorisée.

[0088] Par ailleurs, d'autres zones de confinement sont définies dans le traitement d'erreur autorisé par le dispositif de l'invention :

- confinement temporel des erreurs au niveau d'un cycle temps réel puisque la correction est basée sur une granularité d'un cycle temps réel ;
- confinement des erreurs au niveau des tâches logicielles grâce au dispositif de l'invention de surveillance des accès mémoire et au niveau des chaînes virtuelles également grâce à la surveillance des accès mémoire.

Tables du procédé

[0089] Le fonctionnement du traitement d'erreur autorisé par le dispositif de l'invention s'appuie sur un jeu de tables où sont en particulier stockées les données à voter (ces tables sont donc dupliquées, un jeu étant géré par ChV#1, l'autre par ChV#2). On appelle ces tables « tables du duplex multiplexé dans le temps » car elles sont spécifiques au fonctionnement duplex, par opposition aux tables usuelles du logiciel. On peut citer par exemple :

- table d'acquisition (TAB-Acq),
- table de commande (TAB-Cde),

- table de contexte (TAB-Ctxt).

[0090] Pour permettre une restauration du contexte lors d'une correction par reprise, chacune des tables de contexte TAB-Ctxt#1 et TAB-Ctxt#2 est en fait constituée d'un jeu de deux tables qui travaillent en basculement un cycle sur deux en fin de tâche (i.e. en fin de vote). Un jeu de deux index « Old » (ancien) et « New » (nouveau), mémorisés en mémoire, leur est associé.

[0091] Ainsi, lors du cycle numéro N de la tâche K, pour la chaîne virtuelle 1, la première table est par exemple considérée comme « New » et notée TAB-Ctxt-New#1, la deuxième table est « Old » et notée TAB-Ctxt-Old#1. Si aucune erreur n'est détectée par le vote de la tâche K, le basculement en fin de vote intervient les rôles : la première table devient alors TAB-Ctxt-Old#1, et la deuxième TAB-Ctxt-New#1.

[0092] Les zones « Old » sont interdites en écriture grâce au dispositif de l'invention de surveillance des accès mémoire afin de protéger, par exemple, d'un plan-tage du microprocesseur, le contexte de reprise une fois voté et jugé sain.

Séquencement - duplication temporelle

[0093] Par rapport à l'architecture logicielle de référence définie ci-dessus, le traitement d'erreur autorisé par le dispositif de l'invention impose de ne pas générer les commandes au fur et à mesure de leur calcul comme indiqué à la figure 3, mais de les stocker dans une table en attente du vote (voir figure 5B). Lorsque le traitement est terminé pour les deux chaînes virtuelles, les tables sont votées et ce n'est que si aucune incohérence n'est détectée entre elles que le module de vote génère les commandes : i.e. l'une des deux tables de commande est envoyée par l'unité centrale 40 vers l'électronique de commande 43 par l'intermédiaire du bus 45.

[0094] Le séquencement global du traitement d'erreur autorisé par le dispositif de l'invention, pour une tâche donnée, incluant l'aspect duplication temporelle, est décrit ci-après au vu de la figure 9.

[0095] Cette figure illustre le séquencement du duplex multiplexé dans le temps, selon le traitement d'erreur autorisé par l'invention, et le basculement des tables de contexte.

[0096] Les cycles temps réel sont initialisés par des interruptions temps réel IT-TR.

[0097] Chaque cycle temps réel est constitué des phases suivantes :

- séquenceur/exécutif temps réel (ETR),
- tâche A,
- séquenceur/exécutif temps réel,
- tâche B,

- séquenceur/exécutif temps réel,
- tâche C,
- séquenceur/exécutif temps réel,
- tâche de fond et veille.

[0098] La tâche A consiste, de même que les tâches B et C, comme illustré sur la figure 5B, en :

- acquisition chaîne virtuelle numéro 1,
- traitement chaîne virtuelle numéro 1,
- acquisition chaîne virtuelle numéro 2,
- traitement chaîne virtuelle numéro 2,
- vote et génération des commandes.

[0099] On a les étapes suivantes :

- Pendant le Module « traitement » de la chaîne virtuelle numéro 1 (ChV#1) :
 - acquisition des données pour ChV#1 et stockage dans TAB-Acq#1 ;
 - exécution des traitements associés à ChV#1 à partir de TAB-Acq#1 et TAB-Ctxt-Old#1 ; les résultats de ces traitements sont stockés dans les tables TAB-Cde#1 et TAB-Ctxt-New#1 ; aucune commande n'est générée par l'unité centrale vers les acteurs.
- Pendant le Module « Traitement » de la chaîne virtuelle numéro 2 (ChV#2) :
 - acquisition des données pour ChV#2 et stockage dans TAB-Acq#2 ;
 - exécution des traitements associés à ChV#2 à partir de TAB-Acq#2 et TAB-Ctxt-Old#2 ; les résultats sont stockés dans TAB-Cde#2 et TAB-Ctxt-New#2 ; aucune sortie n'est effectuée par le calculateur.
- Pendant le Module « Vote et génération des commandes », c'est-à-dire comparaison des tables et exécution des actions concernant les tables :
 - comparaison mot à mot de TAB-Cde#1 et TAB-Cde#2 ;
 - comparaison mot à mot de TAB-Ctxt-New#1 et TAB-Ctxt-New#2 ;
 - si aucune erreur n'est détectée, poursuite du processus ; sinon, mise en « standby », c'est-à-dire en veille ;
 - commutation des tables de contexte par chan-

gement d'index : TAB-Ctxt-New remplace TAB-Ctxt-Old et sert de contexte pour le prochain cycle temps réel ;

- réalisation des commandes : l'une des deux TAB-Cde est vidée séquentiellement pour transférer les demandes de commandes vers l'électronique de commande via le bus de données ;
- initialisation des paramètres du duplex multiplexé dans le temps (tables du duplex multiplexé dans le temps, variables de gestion du duplex multiplexé dans le temps).

[0100] Ainsi, à la figure 9, lors du cycle temps réel N+1, le contexte d'entrée de la tâche A est TAB-Ctxt-Old(N) si aucune erreur n'a été détectée lors du cycle temps réel N, cette table contenant en fait les données de TAB-Ctxt-New(N) grâce à la commutation ; sinon, le contexte d'entrée de la tâche A est TAB-Ctxt-Old(N-1), cette table étant identique à la table TAB-Ctxt-Old(N-1) du cycle temps réel N puisque la commutation des contextes n'a pas lieu en cas d'erreur.

[0101] Durant les modules de traitement, un code de contrôle (checksum) est calculé pour chacune des tables qui sont soumises au vote ; il participe à la vérification de l'exhaustivité (de l'intégrité) du vote.

Vote logiciel sécurisé

[0102] Les données qu'il est nécessaire au minimum de voter sont les différentes sorties du module de traitement, comme illustré sur la figure 10, à savoir :

- les données 65 sortant du calculateur (les commandes) pour ne pas générer d'actuators erronées,
- les données 66 servant à la reprise (le contexte : si le cycle N est en faute, les données saines N-1 seront restituées pour la reprise), le contexte de reprise se devant d'être sain.

[0103] Ainsi, toutes les données sortant du module de traitement sont votées. Le vote associé à une tâche donnée est réalisé en fin de cette tâche, ceci étant défini par la granularité de la détection/correction.

[0104] En ce qui concerne le module vote, le traitement d'erreur autorisé par le dispositif de l'invention permet d'obtenir les caractéristiques suivantes :

- Pas besoin d'utiliser un composant externe tolérant aux événements singuliers si l'on sait définir des dispositifs de sécurisation du vote ; l'architecture en est ainsi simplifiée : le vote peut être réalisé par le microprocesseur lui-même, entièrement en logiciel, avec un support des quelques dispositifs matériels formant le dispositif de l'invention.
- Le vote logiciel n'est pas dupliqué.

[0105] Le traitement d'erreur autorisé par le dispositif

de l'invention est basé sur l'utilisation au mieux des capacités de détection d'une architecture duplex, c'est-à-dire pouvant détecter tous les types d'erreur, y compris les erreurs de séquençement qui sont à la fois les plus difficiles à détecter et qui ont potentiellement les conséquences les plus graves. Ces erreurs ont un impact sur la cohérence des tables du duplex multiplexé dans le temps ; elles sont donc détectées par un vote logiciel à condition qu'il soit sécurisé, c'est-à-dire qu'il ne puisse être déclenché par un microprocesseur fonctionnant incorrectement. Il faut donc s'assurer de l'intégrité du vote par des mécanismes adéquats.

[0106] La sécurisation du vote est basée sur deux éléments centraux :

- vérification en début de vote de l'état sain du microprocesseur et du module unité centrale,
- vérification en cours de vote de la complétude du vote, afin d'autoriser la génération des commandes.

[0107] La structure du vote est définie en fonction de l'analyse des possibilités de mauvais branchement d'un microprocesseur victime d'un plantage « doux », la figure 11A illustre les différentes erreurs de séquençement possible de type « plantage doux ».

[0108] Les « plantages durs » sont traités par un chien de garde, méthode usuelle pour l'homme de l'art.

[0109] La structure du module de « Vote logiciel et génération des commandes » associé à la tâche K est illustrée sur la figure 11B est la suivante :

- a) vérification de l'état du microprocesseur se branchant au début du vote et du module unité centrale : vérifier que le pointeur de pile est dans la zone autorisée, vérifier les registres de configuration du microprocesseur et de la carte unité centrale ;
- b) inhibition des caches si possible pour minimiser la probabilité d'erreur durant le vote ;
- c) vérification d'une variable Clé-Vote à 0, puis mise à 1 (i.e. vote) ; cette variable est une clé permettant de contrôler globalement le bon séquençement du microprocesseur grâce à un procédé de Surveillance Logiciel ;
- d) activation de la clé du dispositif surveillance d'accès mémoire indiquant un vote en cours et autorisant l'accès simultané aux deux zones mémoire ChV#1 et ChV#2 ;
- e) vote de toutes les tables résultantes du duplex multiplexé dans le temps et calcul d'un code redondant cyclique calculé lors des votes CRC-V, au fur et à mesure du vote, pour chaque table : TAB-Cde, TAB-Cbt-New ;
- f) vérification de Clé-Vote à 1, puis mise à 2 (i.e. génération des commandes) ;
- g) comparaison des CRC-V aux codes redondants cycliques calculés lors des traitements CRC-T ;
- h) inhibition de la clé du dispositif de surveillance d'accès mémoire indiquant un vote en cours ;

i) si le résultat des tests e, f et g est correct, alors ouverture d'une fenêtre de validation temporelle du coupleur de bus grâce au dispositif de fenêtre de validation temporelle ;

j) réinitialisation des registres de configuration des cartes de commandes ;

k) génération des commandes vers le coupleur de bus ;

l) vérification des registres de configuration des cartes de commandes, et action en fonction du type d'erreur éventuellement détecté (en général : réémission de la commande) ;

la fenêtre temporelle s'est terminée, ou va se terminer ;

m) vérification de Clé-Vote à 2, puis mise à 3 (i.e. commutation et initialisation) ;

n) basculement des tables de contextes de la tâche K en intervertissant son jeu d'index « Old » et « New » stocké en mémoire ;

o) initialisation de toutes les tables de la tâche K, hormis les tables « Old » avec des valeurs en complément à 1 entre ChV#1 et ChV#2 ;

p) transfert des tables « Old » vers les tables « New », et vote pour vérifier ce transfert ; ce transfert est nécessaire pour assurer la pérennité des variables qui ne sont pas mises à jour systématiquement à chaque exécution de tâche ;

q) vérification de Clé-Vote à 3, puis mise à 0 (i.e. inhibé) ;

r) validation des caches.

[0110] La procédure « vote/génération des commandes/commutation/initialisation des tables du duplex multiplexé dans le temps » est non sécable, i.e. elle ne doit pas être préemptée (une fois initialisée, elle doit se terminer). Une interruption peut, par contre, interrompre momentanément ce module.

Processeur de surveillance logiciel

[0111] Un procédé de Surveillance Logiciel, connu de l'homme de métier, permet de confier au logiciel lui-même le contrôle du bon séquençement des instructions du microprocesseur. Le logiciel est découpé en segments élémentaires linéaires, c'est-à-dire compris entre deux branchements. Les segments linéaires ne comportant pas eux-mêmes d'instructions de branchement, une fois que le microprocesseur a exécuté la première instruction de ce segment, celui-ci doit forcément arriver jusqu'à l'exécution de la dernière instruction de ce même segment.

[0112] On vérifie que le microprocesseur est bien rentré dans un segment linéaire exactement à son point d'entrée, et non ailleurs, grâce au prélèvement d'une clé au point d'entrée et son contrôle au point de sortie.

[0113] La sécurisation du vote utilise entre autre ce procédé de Surveillance Logiciel ; la variable logicielle « Clé-Vote » étant une clé associée à ce procédé. Ce

module vote est partitionné en trois segments fonctionnels (vote, génération des commandes, commutation et initialisation), le reste du logiciel applicatif représentant en quelque sorte un quatrième segment :

- en début de chaque segment, on contrôle la valeur de la clé du procédé de Surveillance Logiciel pour s'assurer que le microprocesseur est bien sorti du segment précédent exactement à son point de sortie et non ailleurs, on vérifie ainsi que les segments s'enchaînent bien les uns à la suite des autres ;
- puis, juste après ce contrôle de début de segment, on positionne la clé du procédé de Surveillance Logiciel à une valeur correspondant au segment courant ;
- en fin de chaque segment, on contrôle que le microprocesseur est bien rentré dans le segment courant exactement à son point d'entrée et non ailleurs.

Protection du plan mémoire

[0114] Les plans mémoires sont classiquement protégés contre les événements singuliers par code correcteur (EDAC) et tâche de relecture en tâche de fond de tout le plan mémoire pour détecter et corriger les erreurs dormantes. Ceci est nécessaire car de multiples erreurs sur le même mot ne pourraient plus être détectées et/ou corrigées.

[0115] Le traitement d'erreur autorisé par le dispositif de l'invention s'appuie :

- sur une mémoire fiable vis-à-vis des événements singuliers grâce à l'utilisation d'un code correcteur (EDAC) ;
- sur une mémoire fiable vis-à-vis des écritures incorrectes suite à une erreur d'adresse, d'instruction, un plantage du microprocesseur, etc., grâce à l'utilisation du dispositif de l'invention réalisant une surveillance des droits d'accès.

Dispositif de surveillance des accès mémoire

[0116] Le dispositif de l'invention de Surveillance des Accès Mémoire ou SAM est un dispositif matériel dérivé des classiques unités de protection mémoire par blocs. Il permet de vérifier que le microprocesseur cherchant à accéder à une zone mémoire délimitée, en possède bien le droit d'accès.

[0117] Le dispositif de l'invention de surveillance d'accès mémoire permet de détecter une grande partie des erreurs d'adresses. Il permet, en particulier, de détecter très rapidement de nombreux cas de plantage du microprocesseur. En effet, suite à un plantage « doux », un microprocesseur peut fréquemment sortir de la zone d'adresses autorisée.

[0118] Le dispositif de l'invention de surveillance d'accès mémoire dispose de certaines spécificités par rapport à une unité de protection mémoire par bloc

classique :

- la taille des segments est quelconque, et définie en fonction de l'application ;

5

- l'autorisation d'accès se fait en programmant des clés mémorisées dans des registres internes au dispositif de surveillance d'accès mémoire, la définition et la combinaison de ces clés entre elles étant spécifiques au procédé de l'invention.

10

[0119] La liste des clés intégrées dans le dispositif de surveillance d'accès mémoire est la suivante :

15

- Clé d'interdiction d'accès en écriture à la zone mémorisant le code, car une erreur de code serait une erreur de mode commun aux deux chaînes virtuelles et ne pourrait pas être détectée par le vote. Cette clé permet d'autoriser l'écriture de la mémoire uniquement lors de l'initialisation du calculateur, lorsque le code en mémoire morte est transféré en mémoire vive.

20

25

- Clé indiquant quelle est la chaîne virtuelle courante, ChV#1 ou ChV#2, et interdisant au microprocesseur d'accéder à la zone mémoire contenant les tables de ChV#2 lorsque c'est ChV#1 qui est en train de s'exécuter (et réciproquement). Cette clé permet une étanchéification aux erreurs d'une chaîne virtuelle par rapport à l'autre.

30

- Clé indiquant un vote en cours d'exécution : lorsqu'elle est active, elle autorise exceptionnellement au microprocesseur d'accéder simultanément aux deux zones ChV#1 et ChV#2 pour pouvoir réaliser le vote.

35

- Clé indiquant quelle est la tâche courante, et autorisant le microprocesseur à n'accéder qu'à la zone mémoire contenant les tables de la tâche du logiciel en cours d'exécution. Cette clé permet une étanchéification aux erreurs d'une tâche par rapport aux autres.

40

- Clé indiquant quelle est, parmi les jeux de deux tables « Old »/ « New » travaillant en basculement, les zones « Old » et les zones « New », les zones « Old » étant interdites en écriture.

45

50

Dispositif de fenêtre de validation temporelle

[0120] Le dispositif de Fenêtre de Validation Temporelle ou FVT est un dispositif matériel original. Il est réalisé à l'aide d'un compteur de temps classique. Il permet de confiner les erreurs au niveau matériel. Il est conçu pour :

55

- interdire à un microprocesseur planté qui irait exé-

cuter du code de gestion de l'électronique de commandes, de générer une commande sans avoir acquitté correctement un droit d'accès ;

- interdire à un microprocesseur qui exécuterait une instruction erronée de type « écriture à une adresse correspondant à une commande » de générer une commande par inadvertance.

[0121] Le dispositif de fenêtre de validation temporelle protège donc le système de commandes intempestives, avec les conséquences potentiellement catastrophiques que celles-ci pourraient avoir pour l'application. Il est armé préalablement pour autoriser l'accès à l'électronique de commande : on ouvre une fenêtre de validation d'accès temporelle.

[0122] Dans les cas d'erreurs mentionnés ci-dessus, le microprocesseur n'accède pas à l'électronique de commande en exécutant la procédure d'interface de façon exhaustive ; par conséquent, l'accès non autorisé est immédiatement détecté par ce dispositif puisque le microprocesseur n'a pas ouvert préalablement la fenêtre de validation temporelle.

[0123] Le dispositif de fenêtre de validation temporelle est armé après avoir pris la décision qu'aucune erreur n'était présente. Cette décision est basée d'une part sur la vérification de l'état sain du microprocesseur et de l'unité centrale (en début de vote, puis avec la variable "clé vote" et le contrôle de "checksum" en cours de vote) et d'autre part sur le résultat du vote.

Correction

[0124] La correction s'exécute suivant le séquencement suivant :

- lorsqu'une erreur est détectée, le cycle temps réel courant (numéro N) est inhibé, aucune commande n'est générée : le microprocesseur passe en mode veille en attendant le cycle temps réel suivant,
- le cycle temps réel suivant N+1 s'exécute non pas à partir du contexte N, qui n'est pas sûr, mais du contexte précédent N-1, et des acquisitions du cycle courant N+1.

[0125] On ne rejoue pas le cycle temps réel fautif, on se contente simplement d'inhiber le cycle temps réel courant et de restaurer le contexte du cycle précédent. En cas d'erreur, le microprocesseur ne génère pas les commandes du cycle temps réel courant puisqu'il s'est mis en veille : tout se passe comme s'il y avait un « trou » d'un cycle temps réel.

[0126] La correction ne nécessite aucune action spécifique : le microprocesseur s'étant mis en veille après une détection, il ne poursuit pas l'exécution du module de vote ; cela entraîne naturellement une non permutation des contextes « Old » et « New » qui se fait en fin du module vote.

[0127] Étant donné le caractère transitoire des er-

reurs détectées par le procédé, une seule tentative de reprise est effectuée. Si elle est infructueuse, une réinitialisation complète du calculateur est alors nécessaire.

5 Séquenceur - Exécutif temps réel

[0128] Le séquenceur, ou l'exécutif temps réel, qui permettent l'ordonnancement des tâches logicielles, ne sont pas directement protégés. L'objectif est de pouvoir utiliser un exécutif commercial, donc de ne pas le modifier pour y intégrer des mécanismes de tolérance aux fautes.

[0129] Par contre, le temps d'exécution qui leur est consacré, au regard du temps d'exécution total, est très faible. Par conséquent, les erreurs d'ordonnancement des tâches sont des modes communs aux deux chaînes virtuelles, non détectables, mais qui ont un impact très réduit sur le taux de couverture.

[0130] Par ailleurs, les zones de confinement permettent de bloquer une partie des erreurs non détectées avant qu'une mauvaise commande ne soit initialisée réduisant ainsi l'impact des erreurs provenant, entre autre, de l'ordonnanceur.

25 Variantes de réalisation

[0131] Des variantes du traitement d'erreur autorisé par le dispositif de l'invention sont possibles, en particulier en simplifiant certaines de ses caractéristiques, par exemple.

- Simplification des sécurités du vote : suppression du calcul de somme de contrôle « checksum », le contrôle par procédé de surveillance logiciel étant considéré comme suffisant.
- Simplification du dispositif de l'invention de surveillance des accès mémoire : pas de cloisons étanches entre ChV#1 et ChV#2 (suppression de la clé indiquant la chaîne virtuelle courante), car la probabilité d'erreurs identiques entre les deux chaînes est a priori très faible.

45 Développement et réalisation du traitement d'erreur autorisé par le dispositif de l'invention

[0132] Le traitement d'erreur autorisé par le dispositif de l'invention a été développé dans le but de réaliser une validation la plus générique et la plus exhaustive possible, et d'effectuer une mesure du taux de couverture d'erreur que l'on peut atteindre.

Objectif

[0133] L'objectif recherché était de disposer d'une réalisation (maquette) matérielle et logicielle représentative d'une application spatiale typique, dans le but de valider une fois pour toutes le traitement d'erreur auto-

risé par le dispositif. Un projet spatial en effet analyse, dans les phases préliminaires, les différentes solutions utilisables. Pour les solutions nouvelles, une preuve de bon fonctionnement et d'adéquation au besoin est recherchée à travers une maquette, ce qui entraîne des délais notables avant que l'équipe projet puisse se prononcer sur son utilisation.

[0134] Par conséquent, en avance de phase, une validation générique est entreprise afin de pouvoir fournir, à tout projet intéressé, un dossier complet : spécifications de besoin, spécifications de réalisation, dossiers de réalisation, résultats de validation, résultats de mesure de taux de couverture d'erreurs, etc.

[0135] Ainsi, en phase préliminaire, tout projet peut disposer du dossier complet de développement/validation de ce traitement d'erreur autorisé par le dispositif sans avoir besoin de redévelopper une maquette. Par conséquent, par exemple à travers un audit, il peut déterminer rapidement l'adéquation entre le procédé et le besoin du projet afin de prendre une décision quant à sa sélection.

Méthode de validation

[0136] Le traitement d'erreur autorisé par le dispositif de l'invention est validé par injection de fautes. Deux types d'injection, avec des objectifs distincts, sont ainsi réalisés.

- Dans une première phase, une injection logicielle d'erreurs déterministes est réalisée. Dans la mesure où cette injection est synchrone, il est possible de rejouer les scénarios d'erreurs lorsque le traitement d'erreur autorisé par le dispositif est mis en défaut. Cette phase permet ainsi de valider le traitement d'erreur autorisé par le dispositif, et potentiellement de le faire évoluer afin d'améliorer ses performances de détection/correction d'erreurs.
- Dans une deuxième phase, une injection d'erreurs aléatoires est réalisée en soumettant les composants principaux de la réalisation à un faisceau de particules (ions lourds, protons) dans un accélérateur de particules. Cette phase, complémentaire de la précédente, permet une validation de bout en bout car le spectre des erreurs injectées est plus large. De plus, puisque la distribution des erreurs est représentative d'un environnement applicatif réel, elle permet de mesurer finement le taux de couverture d'erreurs du traitement d'erreur autorisé par le dispositif.

Réalisation matérielle

[0137] La réalisation matérielle développée est constituée principalement de trois parties : l'unité de traitement, l'unité d'acquisition et l'unité d'observabilité.

[0138] L'unité de traitement est développée autour d'un microprocesseur de type Power PC 603e et de sa

mémoire, ainsi que d'un composant programmable intégrant tous les mécanismes matériels du dispositif de l'invention.

[0139] L'unité d'acquisition permet de simuler plusieurs canaux d'acquisition pour le microprocesseur, chacun de ces canaux ayant des caractéristiques particulières : acquisitions effectuées sur demande du microprocesseur (simulation de capteurs simples), acquisitions effectuées cycliquement et que le microprocesseur doit lire à la volée (simulation de capteurs intelligents tel qu'un senseur stellaire ou un GPS), réception de télécommandes, etc. Ces canaux d'acquisition sont réalisés autour de nano-contrôleurs de type PIC 16C73A.

[0140] L'unité d'observabilité intègre la commande-contrôle de la réalisation (chargement du logiciel, observabilité du microprocesseur, etc.) ainsi qu'un canal permettant la simulation des actuations effectuées par le microprocesseur. Les sorties sur ce canal sont systématiquement contrôlées pour vérifier qu'il n'y a pas de fausses actuations générées par le calculateur malgré le fait qu'il soit soumis à des erreurs transitoires.

Réalisation logicielle

[0141] Afin d'être le plus représentatif possible des applications temps réel embarquées, spatiales ou d'autres domaines, le logiciel applicatif développé (i.e. la réalisation logicielle) dispose des caractéristiques suivantes :

- séquençement basé sur un séquenceur cyclique, qui sera ultérieurement remplacé par un exécutif temps réel commercial ;
- plusieurs tâches applicatives principales, par exemple six, de priorités différentes, certaines cycliques, d'autres apériodiques asynchrones ; l'une des tâches étant le coeur du programme de contrôle d'attitude d'un engin spatial ;
- l'application est basée sur des cycles temps réel rythmés par une horloge temps réel, les tâches applicatives ayant des périodicités différentes ;
- plusieurs tâches applicatives, par exemple trois, sont préemptées par des tâches plus prioritaires ;
- le logiciel doit réagir en temps réel à des événements asynchrones externes provenant des canaux d'acquisition.

REFERENCES

[0142]

[1] « La transition vers les pratiques commerciales en composants électroniques : une voie d'innovation majeure » de P. Lay, F. Bezerra, P. Castillan, J.-P. Fortea, R. Lautheret, et M. Barré, (Systèmes et Services à Petits Satellites, Symposium International, 24-28 juin 1996, Annecy, France)

- [2] « L'environnement radiatif spatial » de J.C. Boudnot, (L'Onde électrique, mai-juin 1991, vol.71, n°3, p.62-68)
- [3] « Effet des radiations sur les composants électroniques » de R. Ecoffet, (module IV, §5.4, p. 493-513, du cours « Techniques et technologiques des véhicules spatiaux » du CNES, Cépaduès-Editions, 1998)
- [4] « Operation of commercially-based microcomputer technology in a space radiation environment » de J.N. Yelverton, (AIAA Computing in Aerospace Conference, 9th, San Diego, CA, 19-21 octobre 1993, pages 192-201, référence : AIAA-93-4493-CP)
- [5] « The theory and practice of reliable system design », de D.P. Siewiorek, et R.S. Swarz, (Digital Press, ISBN 0-932376-13-4, 1982, chapitre 3, p. 118-119)
- [6] « Design and analysis of fault tolerant digital systems » de B.W. Johnson, (Addison-Wesley, ISBN 0-201-07570-9, chapitre 3.6, p.134-136, 1988)
- [7] « Experimental evaluation of two concurrent error detection schemes » de M.A. Schuette, J.P. Shen, D.P. Siewiorek, et Y.X. Zhu (Fault Tolerant Computing Symposium, 1986, p.138-143)
- [8] « Fault recovery of triplicated software on the iAPX 432 » de X.Z. Yang, et G. York, (Distributed Computing System, mai 1985, p.438-443).
- [9] « Transient fault tolerance in digital systems » de Janusz Sosnowski (IEEE Micro, vol. 14, N°1, 1er février 1994 (1994/02/01), pages 24-35, XP000433306).
- [10] EP-A-0 133 004
- [11] « A survey of microprocessor architectures for memory management » de Furth B et al. (Computer, US, IEEE Computer Society, Long Beach., CA, US, Vol. 20, N° 3, page 48-67 XP002034222 ISSN : 0018-9162).

Revendications

1. Dispositif de surveillance des accès mémoire dans un calculateur comprenant une unité centrale, réalisée autour d'un microprocesseur, et une mémoire, **caractérisé en ce que** la mémoire est partitionnée en segments, **en ce que** chaque segment a un droit d'accès défini par une fonction logique de tout ou partie des clés disponibles dans le dispositif, le droit d'accès à chacun des segments étant contrôlé en temps réel, et **en ce que** certains segments ont un accès autorisé seulement si le microprocesseur a une très forte probabilité d'être en bon état de fonctionnement, et permettent ainsi un stockage sûr de données critiques.
2. Dispositif selon la revendication 1, dans lequel, en fonction de la programmation des clés disponibles

dans le dispositif, un ensemble de segments joints est accessible, en lecture seule pour certains segments, en lecture/écriture pour d'autres segments.

3. Dispositif selon la revendication 1, dans lequel la taille des segments est quelconque, afin d'être optimisée pour une application donnée.
4. Dispositif selon la revendication 1, dans lequel la définition du jeu de clés disponibles, les fonctions logiques de combinaison de ces clés et la configuration des segments accessibles en fonction de la programmation des clés, sont spécifiques.
5. Dispositif selon la revendication 1, dans lequel l'un des segments dispose d'une autorisation d'écriture accessible selon un état exceptionnel du calculateur, permettant ainsi un stockage sûr de données critiques.
6. Dispositif selon la revendication 1, dans lequel les segments permettant un stockage sûr de données critiques sont groupés par deux, travaillant en basculement.
7. Dispositif selon la revendication 1, dans lequel le contrôle des droits d'accès permet plusieurs configuration d'accès, chaque configuration autorisant l'accès à un ou plusieurs segments non contigus.
8. Dispositif selon la revendication 1, dans lequel le contrôle des droits d'accès permet la sélection des configurations d'accès selon des combinaisons logiques de une ou plusieurs clés.
9. Dispositif selon la revendication 1, dans lequel le contrôle des transferts vers l'électronique de commande vérifie les droits d'accès et limite dans le temps la validité de ces transferts, délimitant ainsi une zone de confinement des erreurs au niveau matériel.
10. Utilisation du dispositif selon l'une quelconque des revendications précédentes dans le domaine spatial.

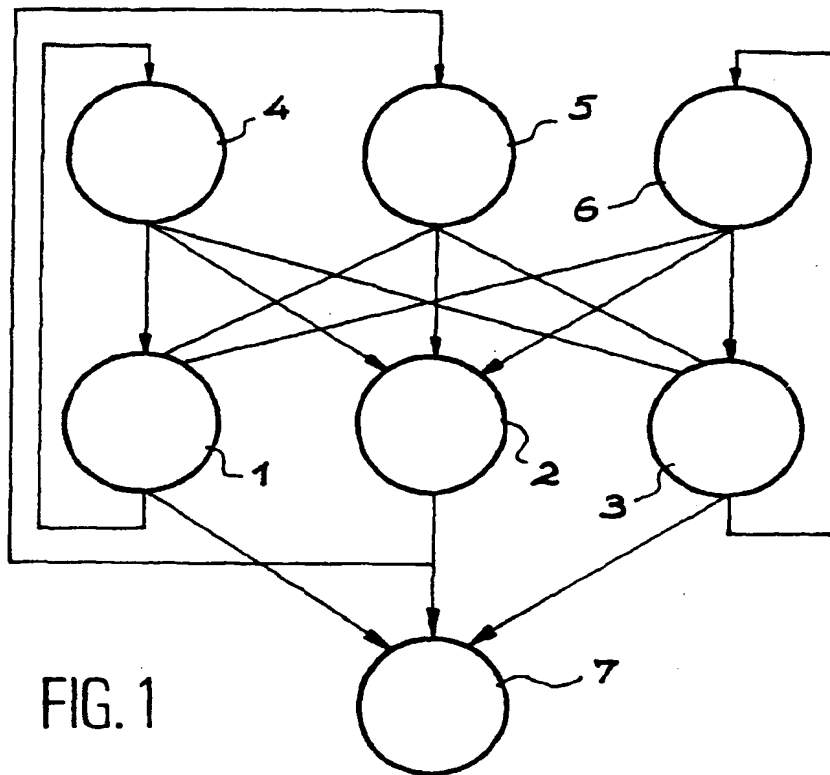


FIG. 1

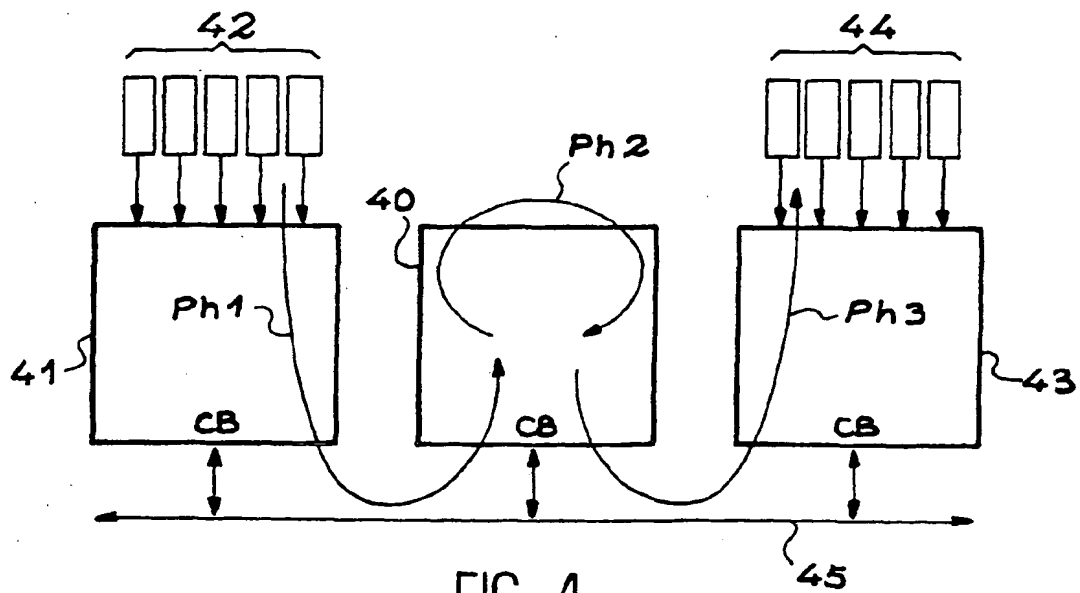


FIG. 4

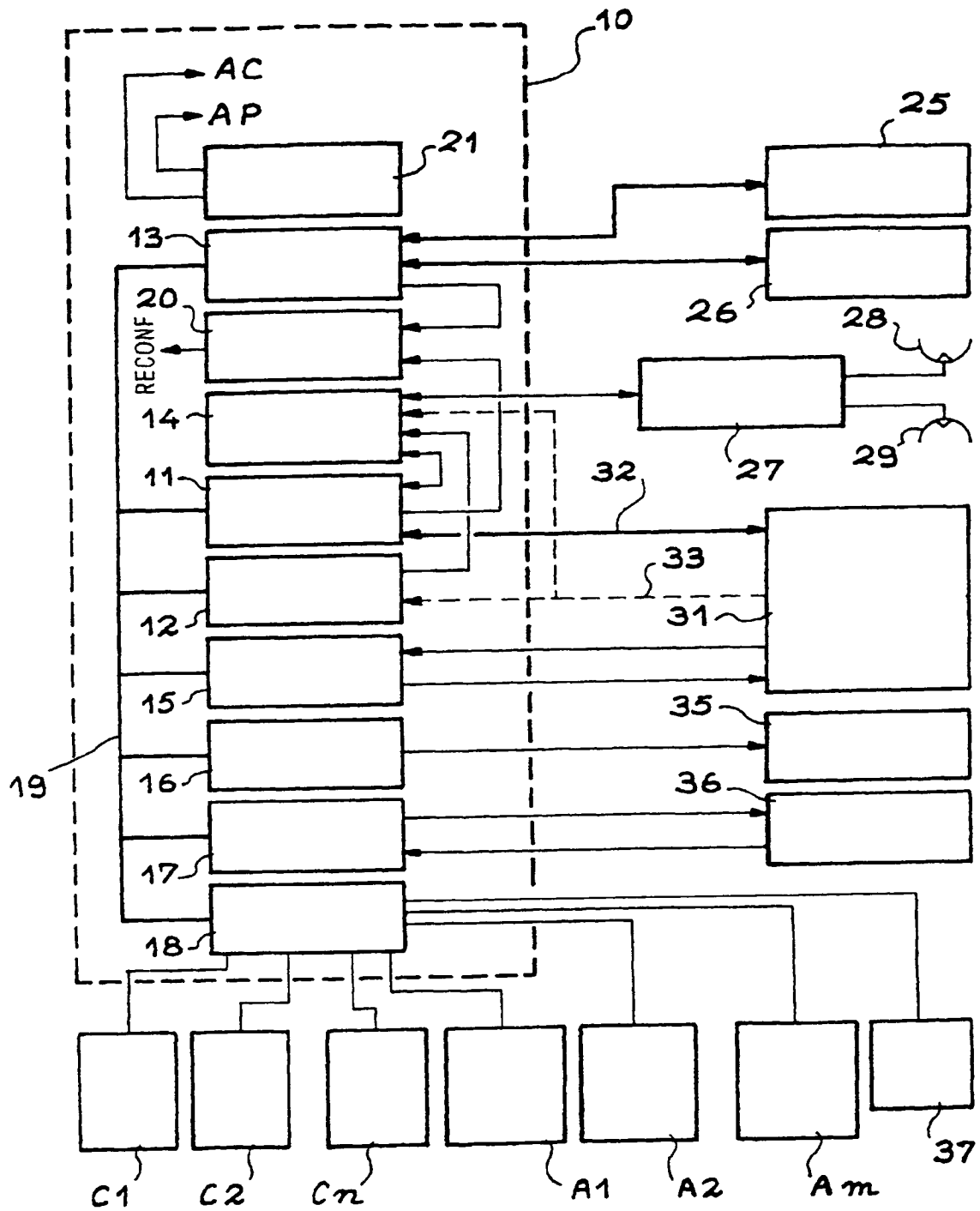


FIG. 2

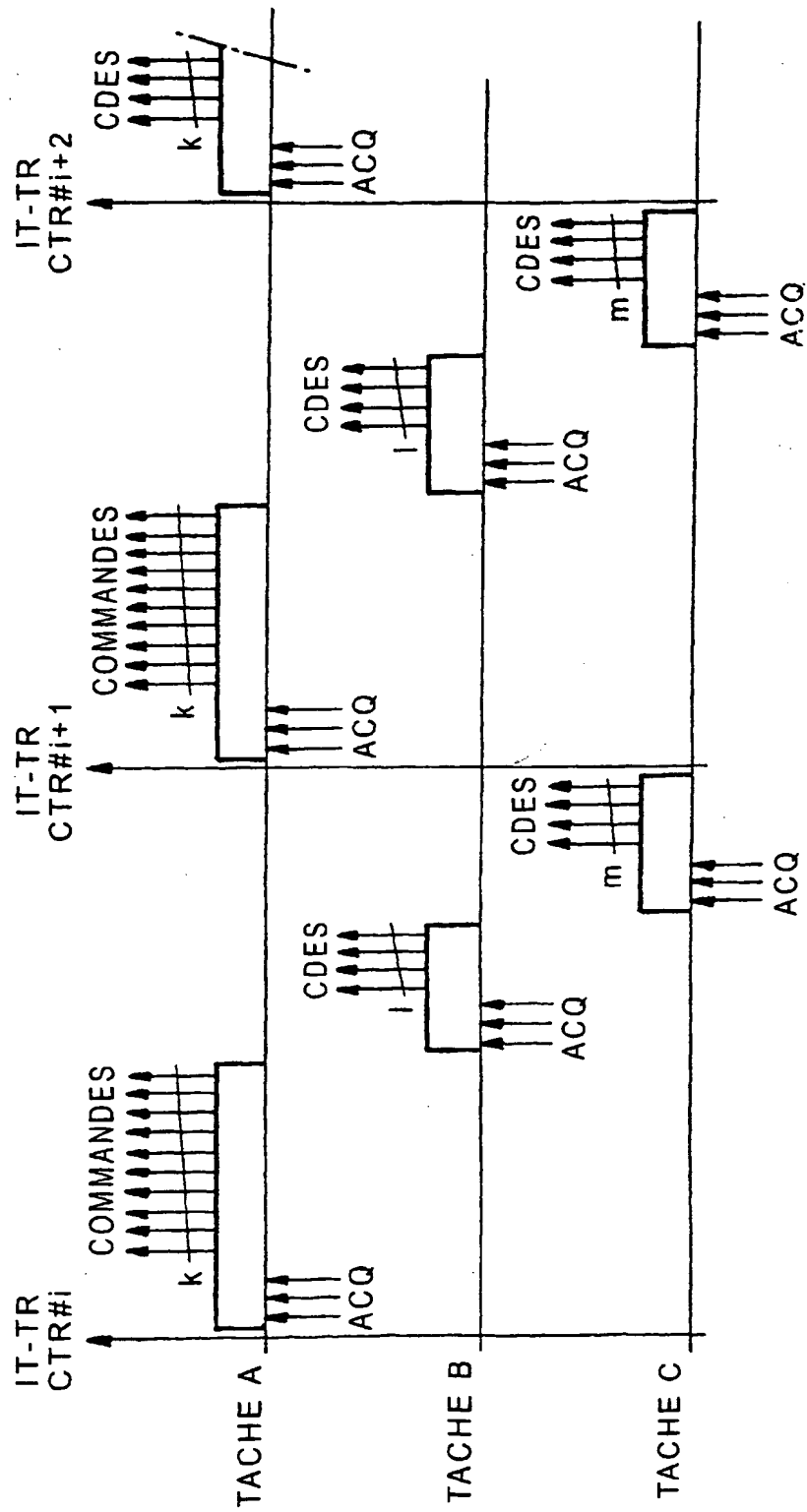


FIG. 3

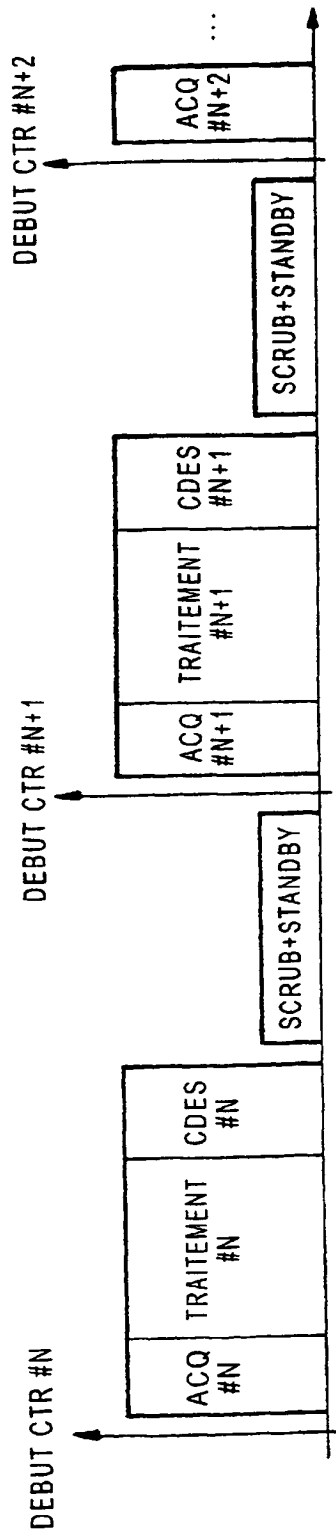


FIG. 5 A

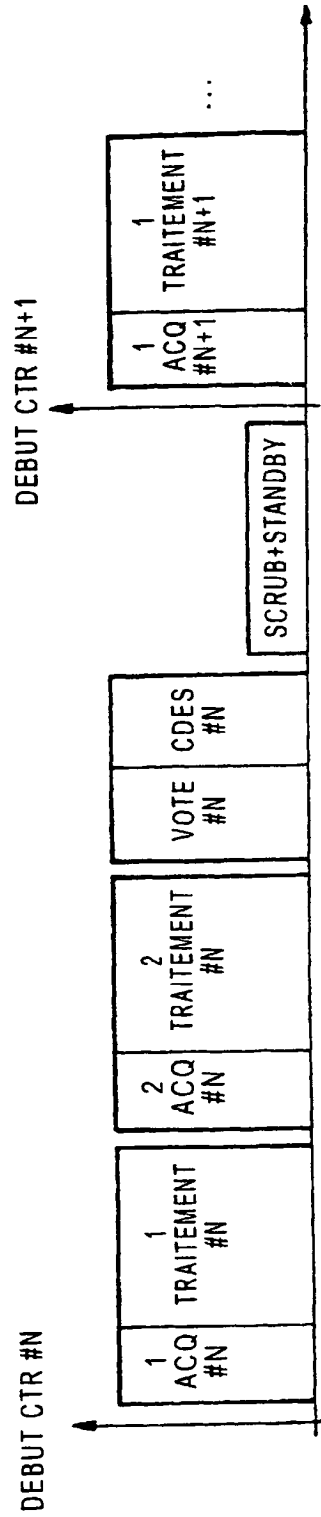


FIG. 5 B

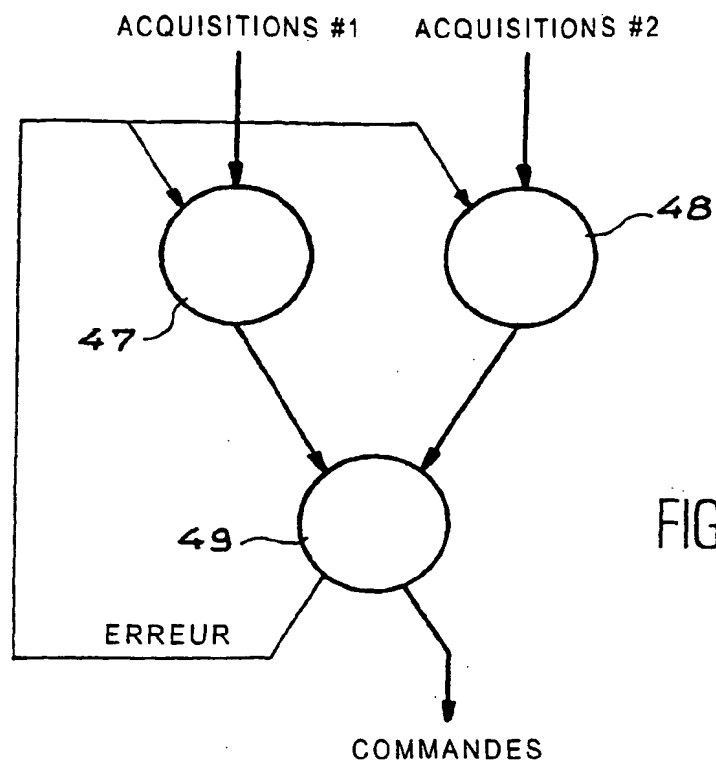


FIG. 6

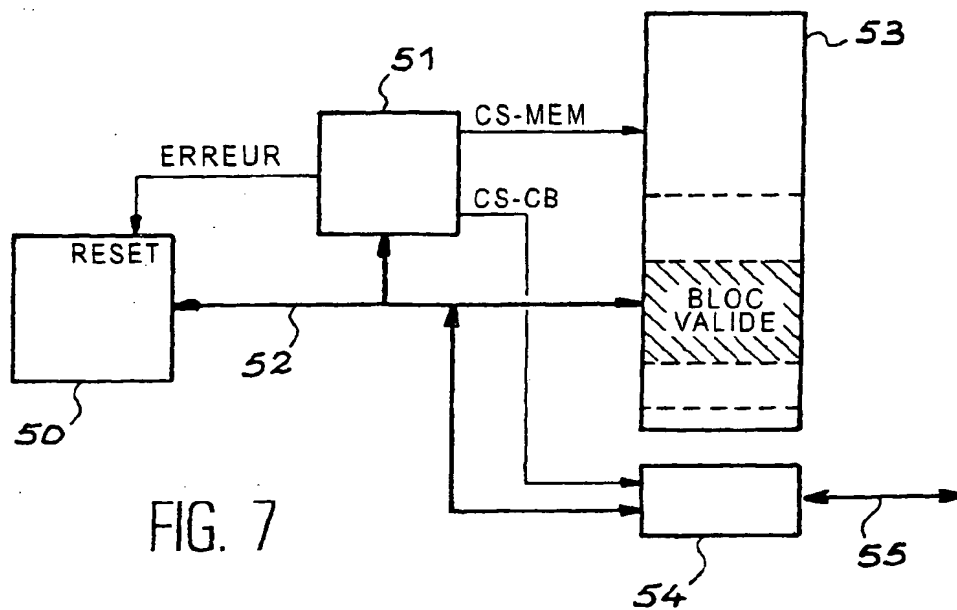


FIG. 7

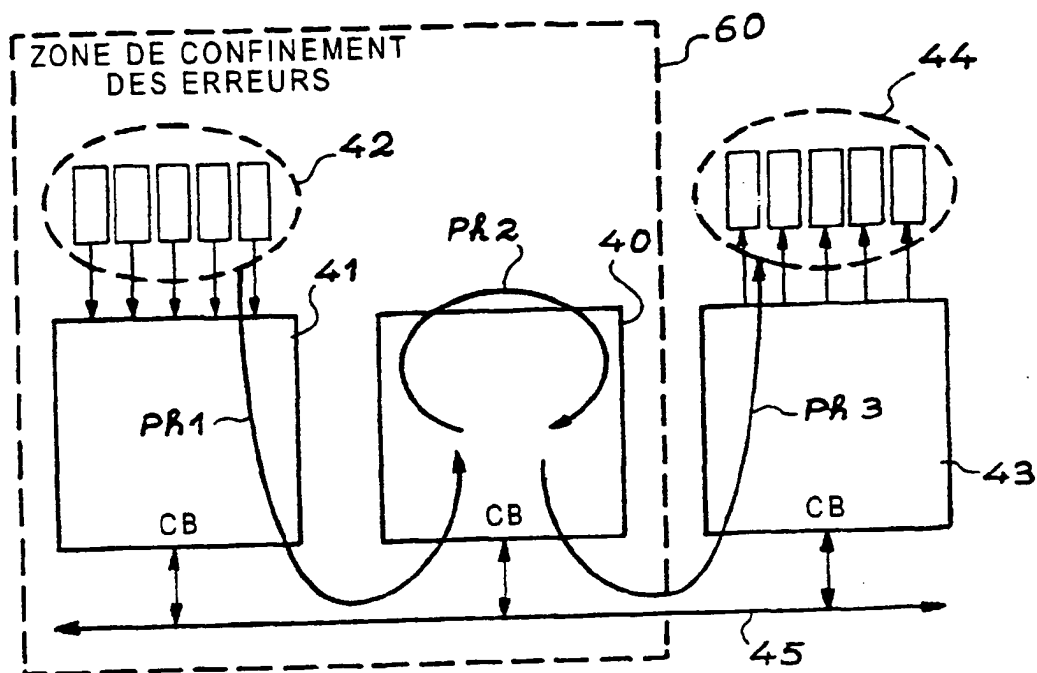


FIG. 8

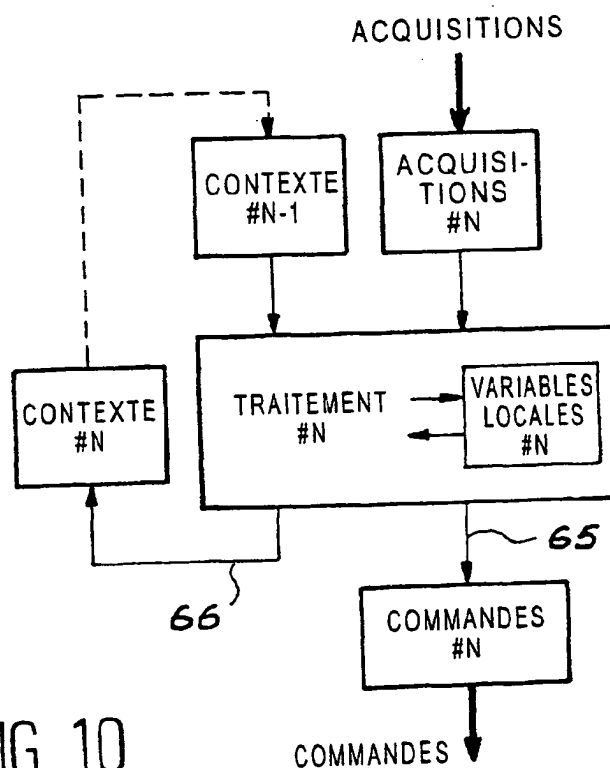


FIG. 10

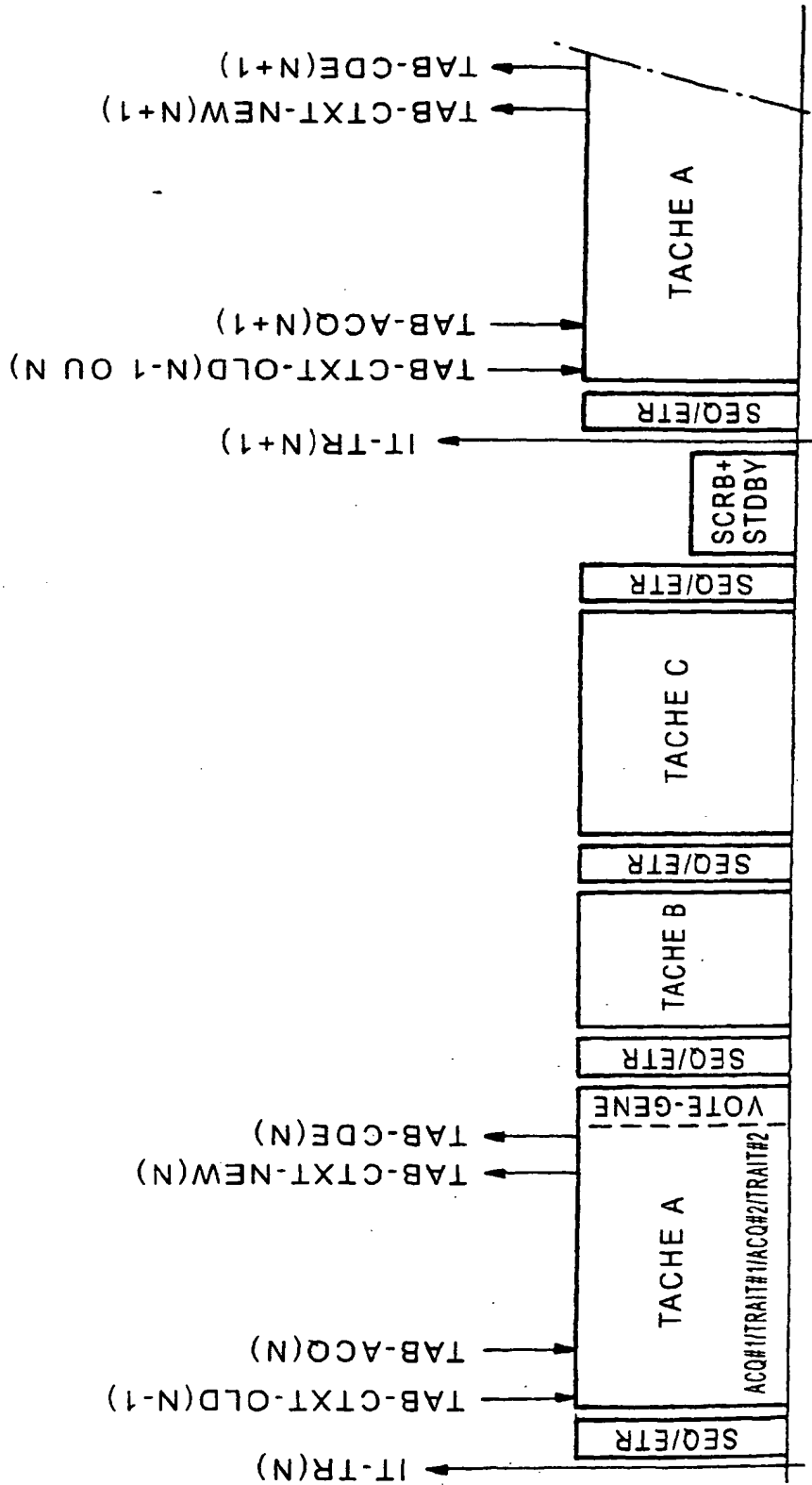


FIG. 9

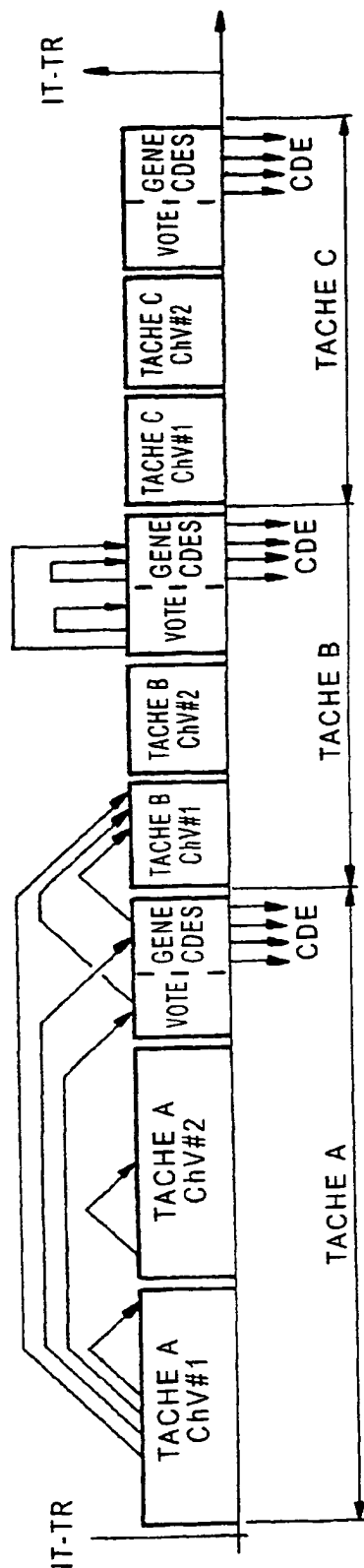


FIG. 11A

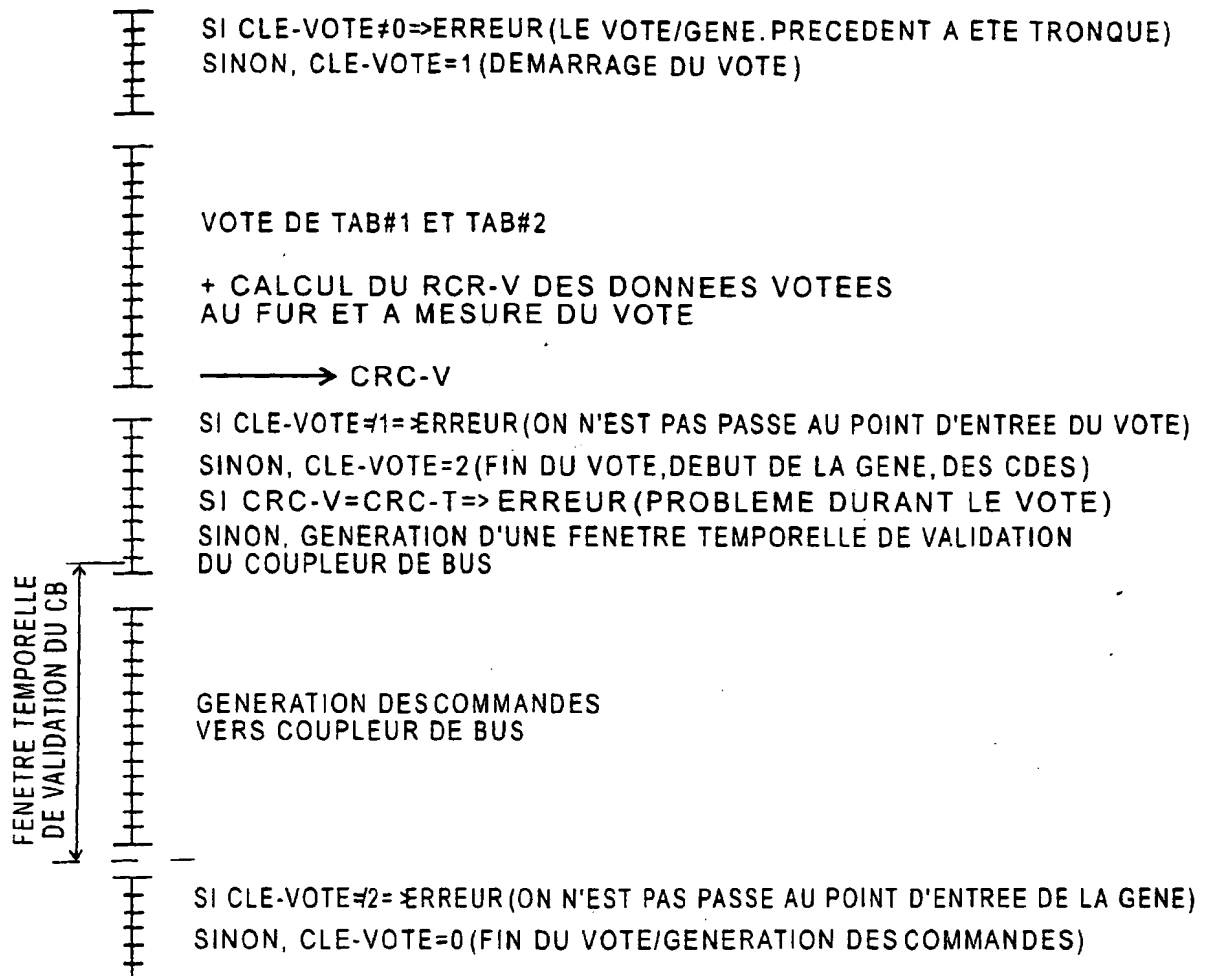


FIG. 11B

THIS PAGE BLANK (USPTO)

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☒ **FADED TEXT OR DRAWING**
- ☒ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☒ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

THIS PAGE BLANK (USPTO)